ID: 382559
Sample Name: 0204_1.gif.dll
Cookbook: default.jbs
Time: 09:54:07
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report 0204_1.gif.dll

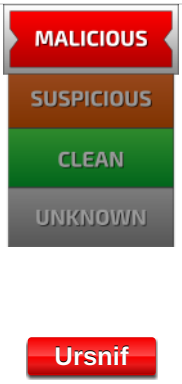
Overview

General Information

Sample Name:	0204_1.gif.dll
Analysis ID:	382559
MD5:	6ebc18a5216386..
SHA1:	6bf2fd63e47f2b2…
SHA256:	65179a35467708..
Tags:	dll GG Gozi ISFB Ursnif
Infos:	

Most interesting Screenshot:

Detection

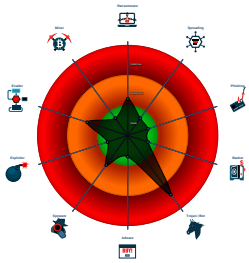


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for subm…
- Yara detected Ursnif
- Yara detected Ursnif
- Machine Learning detection for samp…
- Writes or reads registry keys via WMI
- Writes registry values via WMI
- Antivirus or Machine Learning detec…
- Contains functionality to call native f…
- Contains functionality to dynamically…
- Contains functionality to query CPU …

Classification



Startup

- **System is w10x64**
- loaddll32.exe (PID: 5452 cmdline: loaddll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll' MD5: 542795ADF7CC08EFCF675D65310596E8)
  - cmd.exe (PID: 4904 cmdline: cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll',#1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - rundll32.exe (PID: 68 cmdline: rundll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll',#1 MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
  - rundll32.exe (PID: 2628 cmdline: rundll32.exe C:\Users\user\Desktop\0204_1.gif.dll,StartService MD5: D7CA562B0DB4F4DD0F03A89A1FDAD63D)
- iexplore.exe (PID: 6664 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 6708 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 6972 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:82952 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6780 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 1268 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
  - iexplore.exe (PID: 5188 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17414 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- iexplore.exe (PID: 6384 cmdline: 'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding MD5: 6465CB92B25A7BC1DF8E01D8AC5E7596)
  - iexplore.exe (PID: 3360 cmdline: 'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6384 CREDAT:17410 /prefetch:2 MD5: 071277CC2E3DF41EEEA8013E2AB58D5A)
- **cleanup**

Malware Configuration

Threatname: Ursnif

```
[
  [
    {
      "RSA Public Key":
"Om1HeBhXBR6NHvmWFGSB2kyl5mdcRMsb8ux2uo9VgGW0O2LzHZKk3w9bxw9stgphU0ayytcOYkK6GCNJlKSeMTZJ5WPgZiX+MaXiUccStEUTXkW1ubp0gdr16sb5U4M+rzWWPvc3s7bj9o1yqSJtP7PmMVp7E+3llLULQ9/DZbAD7SXa
ft6wcY8wFj5kI+8D"
    },
    {
      "c2_domain": [
        "bing.com",
        "update4.microsoft.com",
        "under17.com",
        "urs-world.com"
      ],
      "botnet": "5566",
      "server": "12",
      "serpent_key": "10301029JSJUYDWG",
      "sleep_time": "10",
      "SetWaitableTimer_value": "0",
      "DGA_count": "10"
    }
  ]
]
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000003.323251536.0000000004FAB000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000002.486714562.0000000000BE0000.00000004.00000001.sdmp	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
00000001.00000003.318966853.0000000003B2B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000001.00000003.318950554.0000000003B2B000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
00000005.00000003.480525805.0000000004DAF000.00000004.00000040.sdmp	JoeSecurity_Ursnif	Yara detected Ursnif	Joe Security	
Click to see the 16 entries				

Unpacked PEs

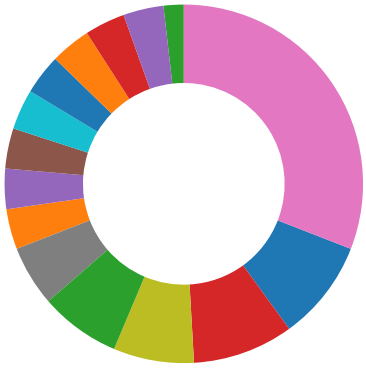
Source	Rule	Description	Author	Strings
4.2.rundll32.exe.bd0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.2ed0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.be0000.1.raw.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
1.2.loaddll32.exe.10000000.4.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	
5.2.rundll32.exe.10000000.5.unpack	JoeSecurity_Ursnif_1	Yara detected Ursnif	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Compliance
- Spreading
- Networking



- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected Ursnif
- Yara detected Ursnif

E-Banking Fraud:

- Yara detected Ursnif
- Yara detected Ursnif

System Summary:

- Writes or reads registry keys via WMI
- Writes registry values via WMI

Hooking and other Techniques for Hiding and Protection:

- Yara detected Ursnif
- Yara detected Ursnif

Stealing of Sensitive Information:

- Yara detected Ursnif
- Yara detected Ursnif

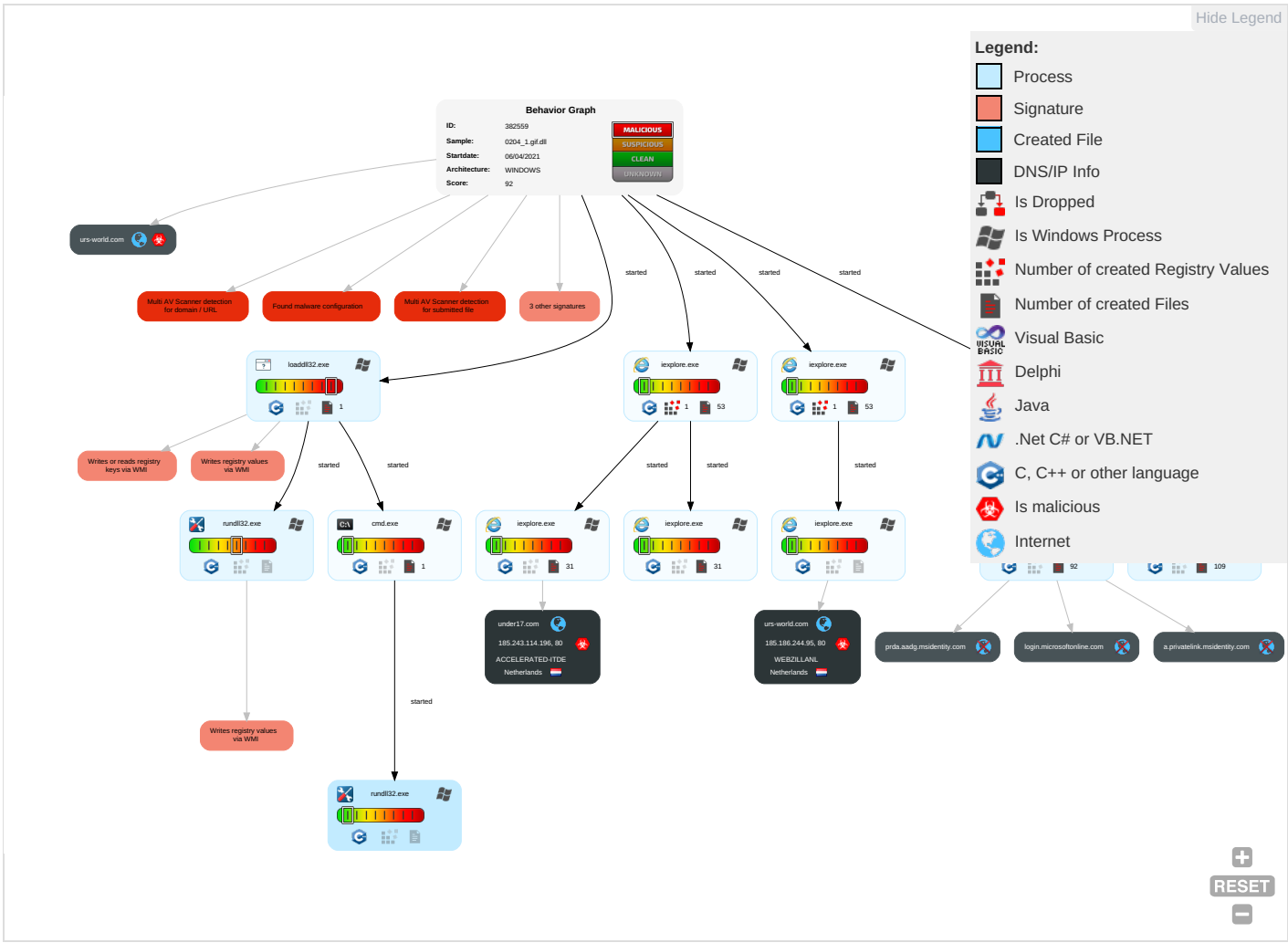
Remote Access Functionality:

- Yara detected Ursnif
- Yara detected Ursnif

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Rem Serv Effe
Valid Accounts	Windows Management Instrumentation 2	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Rem Trac With Auth
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	Rem Wipe With Auth
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obta Devi Clou Bacl
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Rundll32 1	NTDS	Account Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Owner/User Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service	
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points	

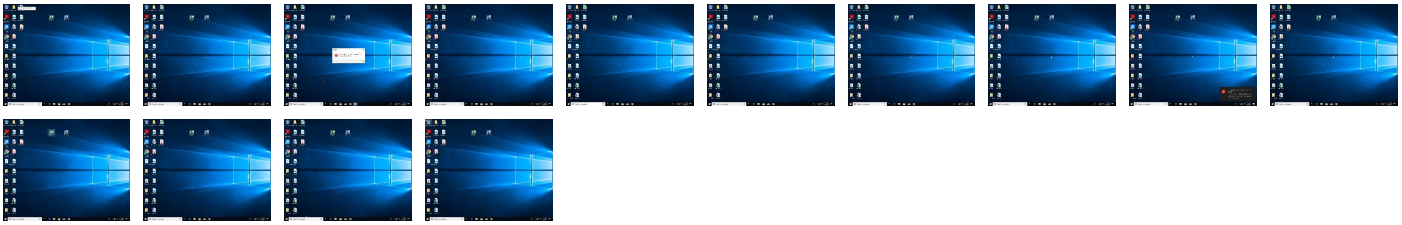
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
0204_1.gif.dll	54%	ReversingLabs	Win32.Trojan.Sdum	
0204_1.gif.dll	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.loaddll32.exe.2f90000.2.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.2d70000.3.unpack	100%	Avira	HEUR/AGEN.1108168		Download File
5.2.rundll32.exe.10000000.5.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File
1.2.loaddll32.exe.1200000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen3		Download File
1.2.loaddll32.exe.10000000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
urs-world.com	6%	Virustotal		Browse
under17.com	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://under17.com/joomla/7ilxUUc2eQiB_2BWW/6r_2BMwbjonk/83d_2FHHC15/HJRFbBiTdFKAEO/luoufpwcpxd9B2Df	0%	Avira URL Cloud	safe	
http://under17.com/joomla/5Ee9Djbm01gK/tl8o1rQRrf7/ve4VcCWGPHbKdt/oB2JQB1Ds_2Fi7cV4n7xM/odh0a6MBnYBo	0%	Avira URL Cloud	safe	
http://urs-world.com/joomla/swXAVHGoBGvGk1d/ryn6afaNNl5GqYjk6D/Ylnh1Zekh/Fo40Y2SBz206KbWZIB4F/dye0VS	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
urs-world.com	185.186.244.95	true	true	• 6%, Virustotal, Browse	unknown
under17.com	185.243.114.196	true	true	• 6%, Virustotal, Browse	unknown
login.microsoftonline.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/nachrichten/politik/l	msnpopularnow[1].json.14.dr	false		high
http://under17.com/joomla/7ilxUUc2eQiB_2BWW/6r_2BMwbjonk/83d_2FHHC15/HJRFbBiTdFKAEO/luoufpwcpxd9B2Df	{FBAD85D8-96F8-11EB-90E4-ECF4BB862DED}.dat.28.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/news/other/das-grosse-impfen-beginnt-geht-es-nun-endlich-vorw	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/janet-yellen-us-finanzministerin-fordert-weltweite-mi	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/so-tickt-kosovos-neue-staatspr	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/es-h	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/vermischtes/die-altersheime-hat-man-vergessen/ar-BB1fkRPW?ocid	msnpopularnow[1].json.14.dr	false		high
http://under17.com/joomla/5Ee9Djbm01gK/tl8o1rQRrf7/ve4VcCWGPHbKdt/oB2JQB1Ds_2Fi7cV4n7xM/odh0a6MBnYBo	~DF4EC0ACC0598C2A74.TMP.28.dr, {FBAD85DA-96F8-11EB-90E4-ECF4BB862DED}.dat.28.dr	false	• Avira URL Cloud: safe	unknown
http://https://www.msn.com/de-ch/nachrichten/politik/das-alles-h	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/alexej-nawalny-klagt-	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/manfred-weber-nennt-eu-beitritt-der-t	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/coronakrise-laschet-fordert-harten-br	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/news/other/der-westen-muss-mit-sanktionen-drohen-die-wehtun/ar-BB1flkV9?oc	msnpopularnow[1].json.14.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.msn.com/de-ch/news/other/polizei-sucht-mit-superpuma-nach-vermissten-minderj	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-a	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/politik/fdp-nur-keine-option-von-vornherein-ausschlie	msnpopularnow[1].json.14.dr	false		high
http://https://login.microsoftonline.com/common/oauth2/authorize?client_id=9ea1ad79-fdb6-4f9a-8bc3-2b70f96e	~DF9401D896BB639998.TMP.13.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/ukrainekonflikt-maas-warnt-russland-und-ukraine-	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/nachrichten/international/admirale-begehren-auf-gegen-das-verr	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/news/other/ressourcen-f	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/finanzen/top-stories/datenleck-bei-facebook-wachstum-z	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/news/other/auf-schmusekurs-mit-erdogan-eu-spitzen-reisen-in-die-t	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/news/other/neuseeland-und-australien-starten-quarant	msnpopularnow[1].json.14.dr	false		high
http://https://www.msn.com/de-ch/news/other/pentagon-usa-beobachten-russlands-aktivit	msnpopularnow[1].json.14.dr	false		high
http://feross.org	GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js.14.dr	false		high
http://urs-world.com/joomla/swXAVHGoBGvGk1d/ryn6afaNNl5GqYjk6D/Ylnh1Zekh/Fo40Y2SBz206KbWZIB4F/dye0VS	{12812620-96F9-11EB-90E4-ECF4BB862DED}.dat.38.dr	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.243.114.196	under17.com	Netherlands		31400	ACCELERATED-ITDE	true
185.186.244.95	urs-world.com	Netherlands		35415	WEBZILLANL	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382559
Start date:	06.04.2021
Start time:	09:54:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0204_1.gif.dll
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal92.troj.winDLL@21/108@9/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 57.9% (good quality ratio 54.7%) • Quality average: 78.8% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 86% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .dll

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, ielowutil.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 92.122.145.220, 40.88.32.150, 104.42.151.234, 104.43.139.144, 88.221.62.148, 184.30.20.56, 13.107.21.200, 204.79.197.200, 131.253.33.200, 13.107.22.200, 40.126.26.133, 40.126.26.135, 20.190.154.17, 40.126.26.132, 20.190.154.139, 40.126.26.134, 20.190.154.138, 20.190.154.16, 20.190.160.134, 20.190.160.2, 20.190.160.4, 20.190.160.129, 20.190.160.69, 20.190.160.73, 20.190.160.6, 20.190.160.132, 20.190.160.1, 20.190.160.130, 20.190.160.74, 20.190.160.131, 20.190.160.7, 20.190.160.9, 20.190.160.72, 20.190.160.70, 20.82.210.154, 93.184.221.240, 92.122.213.194, 92.122.213.247, 152.199.19.161, 13.64.90.137, 52.155.217.156, 20.54.26.129, 168.61.161.212, 52.255.188.83, 52.147.198.201 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, www.tm.a.prd.aadg.trafficmanager.net, e11290.dspg.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, login.live.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, wst.current.a.prd.aadg.trafficmanager.net, blobcollector.events.data.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net, cs9.wpc.v0cdn.net, store-images.s-microsoft.com-c.edgekey.net, bing.com, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, iecvlist.microsoft.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, go.microsoft.com, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, www2.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, ie9comview.vo.msecnd.net, wu.ec.azureedge.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, login.msa.msidentity.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, www2-bing-com.dual-a-0001.a-msedge.net, go.microsoft.com.edgekey.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.243.114.196	gg.gif.dll	Get hash	malicious	Browse	
	gg_1.gif.dll	Get hash	malicious	Browse	
	gg_2.gif.dll	Get hash	malicious	Browse	
	KcFVz0y2si.dll	Get hash	malicious	Browse	
	bTjvWUTLid.dll	Get hash	malicious	Browse	
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	
	swlsGbeQwT.dll	Get hash	malicious	Browse	
	document-1048628209.xls	Get hash	malicious	Browse	
	document-1771131239.xls	Get hash	malicious	Browse	
	document-1370071295.xls	Get hash	malicious	Browse	
	document-69564892.xls	Get hash	malicious	Browse	
	document-1320073816.xls	Get hash	malicious	Browse	
	document-184653858.xls	Get hash	malicious	Browse	
	document-1729033050.xls	Get hash	malicious	Browse	
	document-540475316.xls	Get hash	malicious	Browse	
	document-1456634656.xls	Get hash	malicious	Browse	
	document-1376447212.xls	Get hash	malicious	Browse	
	document-1813856412.xls	Get hash	malicious	Browse	
	document-1776123548.xls	Get hash	malicious	Browse	
	document-684762271.xls	Get hash	malicious	Browse	
185.186.244.95	document-1048628209.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1771131239.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-69564892.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1813856412.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1776123548.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-647734423.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1579869720.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-806281169.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-839860086.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1061603179.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-909428158.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1822768538.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-1952275091.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico
	document-583955381.xls	Get hash	malicious	Browse	• urs-world .com/favicon.ico

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1312908141.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1612462533.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1669060840.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-203135823.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-1042699213.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico
	document-980795635.xls	Get hash	malicious	Browse	• urs-world.com/favicon.ico

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
urs-world.com	gg.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.186.244.95
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.186.244.95
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1729033050.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-895003104.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-779106205.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
under17.com	gg.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1813856412.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1776123548.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-684762271.xls	Get hash	malicious	Browse	• 185.243.114.196

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACCELERATED-ITDE	gg.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_1.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	gg_2.gif.dll	Get hash	malicious	Browse	• 185.243.114.196
	KcFVz0y2si.dll	Get hash	malicious	Browse	• 185.243.114.196
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.243.114.196
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	BnJvVt951o.exe	Get hash	malicious	Browse	• 152.89.236.214
	SMtbg7yHyR.exe	Get hash	malicious	Browse	• 152.89.236.214
	KAsJ2r4XYY.dll	Get hash	malicious	Browse	• 185.243.114.196
	swlsGbeQwT.dll	Get hash	malicious	Browse	• 185.243.114.196
	document-1048628209.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1771131239.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1370071295.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-69564892.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1320073816.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-184653858.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1729033050.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-540475316.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1456634656.xls	Get hash	malicious	Browse	• 185.243.114.196
	document-1376447212.xls	Get hash	malicious	Browse	• 185.243.114.196
WEBZILLANL	gg_2.gif.dll	Get hash	malicious	Browse	• 185.186.244.95
	bTjvWUTLid.dll	Get hash	malicious	Browse	• 185.186.244.95
	document-1048628209.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1771131239.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-69564892.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1813856412.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1776123548.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-647734423.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1579869720.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-806281169.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-839860086.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1061603179.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-909428158.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1822768538.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1952275091.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-583955381.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1312908141.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1612462533.xls	Get hash	malicious	Browse	• 185.186.244.95
	document-1669060840.xls	Get hash	malicious	Browse	• 185.186.244.95

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	document-203135823.xls	Get hash	malicious	Browse	• 185.186.244.95

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{1281261E-96F9-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.013406639102966
Encrypted:	false
SSDEEP:	192:r9ZjZz2UWsOtsCfsxRMslsLosV/MspMs4sk0uYqy6g:rTlKD9zjycoJVXIq+
MD5:	4ABE06BA7B45F1438327592921172949
SHA1:	9708A6B5CA07882D0F3BCA6CED95A9E9855E0FAD
SHA-256:	323461B8160A0CE30F7CF58165CA85FF37FB5A3A7D2F33BA6322222E43EB361D
SHA-512:	D0CB0711627EBADABF7321B582C9DC1F95E6254389C0D02BECB1AC4D62C8FF0E3CBF59E9104A1557AA192EC61EB7CAEC2045E23D4934AF58879C17765F2D38 86
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{DFDEB0F6-96F8-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.0118121284484216
Encrypted:	false
SSDEEP:	192:r6ZHZq20WBtHSfxhlMPsE/Mr9FfQu3ZWg:rm5JjzwOPsFr9Rb
MD5:	C51E86AA2AFCB1D6667540A905EB73D5
SHA1:	616262B5F96E6182A4D91D2ACC14A0764A6965AD
SHA-256:	3564BBAF2190A697F967C2DF1F2AA5BDE1E43F3C9093F0E09D89F33D67B5A5E4
SHA-512:	8100E17B462AAA4D94853B8494AA288D6DAFF6F950368677B022E19D69D30CBBAC007FD8391E2EF01592B39F5D85306F2BE859D07001DFC7808C00F1C3E4D830
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FBAD85D6-96F8-11EB-90E4-ECF4BB862DED}.dat

Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	50344
Entropy (8bit):	2.007150153486176
Encrypted:	false
SSDEEP:	192:rFZVZFC2Fy1WFy+JBtFy+JphfFy+Jp9xhMFy+JZF9FFy+JZO995KpFy+JZO995K6:rLb3JLHQDJaQjKoc
MD5:	2C9C2CD95631B1B2B0B61A5AAD98756F
SHA1:	617BE4C69D2A0C0138F4C4F20CF6616FDA0404C3
SHA-256:	D9D0CB92AD66BB02D2C198236868560AFBEC71A4BEE6D86E327EE9D0F7008828
SHA-512:	EBAFD628BAF54680A2C0C6E59BE4C3C2561FFA370F76F20F1B0746F839855B8B89D40D41A63184A5DF24768B03F1D0477DCEE48C671F60D5549DAF6C1854424
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{FBAD85D6-96F8-11EB-90E4-ECF4BB862DED}.dat	
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{12812620-96F9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27864
Entropy (8bit):	1.826929920882411
Encrypted:	false
SSDEEP:	96:risZM9Qf6VBSxjx2NWOMqSnOeHatgRn71RnOeHatgRn7aeHatKqr:rlZ+Qf6Vkxjx2NWOMqS7bR7sr
MD5:	4F174BD1BEC86D583CE7D42D2CDF829F
SHA1:	4F1FBCE16CF9C2282A85EB40DA4546F906217F84
SHA-256:	CF4766415E6E0CF68BB77D6B67CAC8EEA89A5A0086689F8B6D2191014AC55A1B
SHA-512:	F9BAE503B957D72D2A31E0C56DAFC099DA852E5429E438F4F7958D4868A2D7FF8D9D425EBCF2D6885553318466263 75F7482DFBB0B6329FD6D50E6E1780AF72A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{12812622-96F9-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.8259468264078385
Encrypted:	false
SSDEEP:	96:rZZKQ+60BSTj920WAMcS5gcBRR5gcBOcBTGr:rZZKQ+60kTj920WAMcSKyRRKyOyar
MD5:	FD39C92A5639AE93B8AD5691AD5018E3
SHA1:	BA7CC9DD826B19AE49F144544796EDA3E5422968
SHA-256:	C70E2F9D528C4E6C62F61C75FF8B4C05FC9A66452D415E0783DDA0A5A82D2801
SHA-512:	18C29716B1ED39BAE21007CFB99A8677C1A34A2A41822E84A3B8EC66E72BD7C1BA5253D8AF9277E17D51473BD8A904936177A3E99744201D3C039AA8B1C9E8A
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DFDEB0F8-96F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	43212
Entropy (8bit):	2.493768127893704
Encrypted:	false
SSDEEP:	384:rjHpx7Mk+w1Gpb4jlWgfiOfiRZfiZvErPxGLPfkYt86a:FioiPiFK
MD5:	D1FD1198431AC8BBDB64A0A574BDB5AC
SHA1:	9020DB0663B94B1787A840939198CE6558B8D24A
SHA-256:	9C42DA02310D54AD58406FFF3E16C3652F2E7C17E0740DDEE6D94D93AB5CE170
SHA-512:	F0CD29B25BDAA9052BF517B596EAC5108DF249F6EACF41BB05660AA3F05B24247ACE8708908A23B7D7CCA37554AE4E1C19EDF50147602799FB9702634C0E76C1
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DFDEB0FA-96F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	41262

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{DFDEB0FA-96F8-11EB-90E4-ECF4BB862DED}.dat	
Entropy (8bit):	2.388184251102208
Encrypted:	false
SSDEEP:	192:roZXQD6lkojh2VWWMPmsGB8AMew7vtkut5I/bWHlOtr:roAmuqQs/ePzYMM8
MD5:	55A2CA485D9DD9E692BB5C5606BD9F68
SHA1:	156A10D0A04CC000CE951AA96BF4BEB97FFCABC5
SHA-256:	3DB56C53062F7E2C0AB25733A2088267921C0462D0D5D867F6E28BBAE843305D
SHA-512:	D7B4235EC6DBFEA1B468EFF88128680E1836D7C86AC9C79F371406ED913C19A0A6DC9F4A674B0343E48945FA5EEA63F18121E7CB888D582AF11BC0438F00852
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FBAD85D8-96F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	dropped
Size (bytes):	27864
Entropy (8bit):	1.826716630641404
Encrypted:	false
SSDEEP:	96:rkZfQb6ZBSr6jC2yWPMXS6WmtjWUR6WmtjW+W0r:rkZfQb6ZkmjC2yWPMXSjmtjNRjmtj20r
MD5:	95ECDF664AB6D3FCA8089F3598F4B840
SHA1:	CD1DB74AE24C3273575DA20954451C55214DA499
SHA-256:	651C3C085B74763C87B263E7FE063D7EAACDCE15D43228319CEA389C31ADB1A5
SHA-512:	3CE80DBEC8BDACA2BBBA677BB282E7E584088A1A53B1155D1DEDE5CF900AEF9F7256BAB3F48DB26487DEAFBDEEE5E4A83803732ACA6DB63A2552E3B5D246 8A64
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{FBAD85DA-96F8-11EB-90E4-ECF4BB862DED}.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	Microsoft Word Document
Category:	modified
Size (bytes):	27340
Entropy (8bit):	1.831586598627649
Encrypted:	false
SSDEEP:	96:r6Z9Qm6QBSgj/A2/+W/oM/4eVGg8OmxVGg8OQHwA:r6Z9Qm6Qkgjo22WAMAeL2xL4wA
MD5:	E4A64C87AA1114EE648ABBB6B62096DF
SHA1:	B6335699B0A285C55CD239DD01DFAFB2A554A63F
SHA-256:	047FAA53E004D908157AA03016429100FCCF495C6CC0CABC2791F1D30183A503
SHA-512:	ECB6659FE893071E3E3587BB9C8E1FEEB63D354625447ABC0EA6B576066A085DF5C788F370CF61DD967022727C8EBB06754A2FEA0D74532755E593F92444216F
Malicious:	false
Preview:	....R.o.o.t. .E.n.t.r. y..... .....

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	10192
Entropy (8bit):	4.533426903978944
Encrypted:	false
SSDEEP:	96:0Ph+Qhato4xfDehrmlPh+Qhato4xfDehrmM:0Z+dn5DehKlZ+dn5DehKM
MD5:	6175CD55831296F2E5A3E44392DFA5BA
SHA1:	57C5EC7F84EC0E622118072FFDAF7600BB7AA014
SHA-256:	F5A8D697906FC0B183EA6C421B55EB303DFBF3E81D746505F8160B847918BC83
SHA-512:	53A93AAAA54BCD2D4666FE5BB413859C8F90D23FECF494B8D078784E090F5BA5D16FB993E42C77EAA3A29A0C5A9E0617B0B6E0AD793C8D72CAB0B6F2289614 75
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Internet Explorer\imagestore\ynfz0jx\imagestore.dat	
Preview:	+.h.t.t.p.s.:././.w.w.w...b.i.n.g...c.o.m./.s.a./.s.i.m.g./.f.a.v.i.c.o.n.-.2.x...i.c.o..... ....(... ...@..... .....N...Sz..R...R...P...N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S...R...P...N..L..I..F..C...?..:z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\FHHVYHNT.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	dropped
Size (bytes):	60841
Entropy (8bit):	5.760027881342484
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQhqETOuKsIecFXdAjvd894fJLYvrMlyb097Q53Opw:GGLQw3f/mQhbd89RLew
MD5:	03E9A7BE6A2D58BAA4CADB8B9C1C86EC
SHA1:	0CA5CD53B3EBF1C728A650E1FAF2C1149A90CD3E
SHA-256:	C8237161315E1618CEACBE522BB4E3B305D36930775006339B3858ADE9B76E64
SHA-512:	79E16CC0FA28ACD66EBA8C3FBADCF89D414656E3C3AA2A5458A1FB0AA9570FE7645996698969921B62ACA6E0F358E8A0CEF4149C6C8219E5064C8AB4CD12B60D
Malicious:	false
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\HdepnBaFj-yarvouFUIlfV4Q9D8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	3201
Entropy (8bit):	5.369958740257869
Encrypted:	false
SSDEEP:	48:rmo6TIPx85uuYPXznTBB0D6e7htJETfD8QJLxDO7KTUx42Z3rtki:sYuYPXznb0DR7dw8QhIWTQrt7
MD5:	4AADD0F43326BAD8EFD82C85B6D9A20E
SHA1:	4093FC4AB9821B646D64C98051A1CF0679CB2188
SHA-256:	968849A1E6AAED249C78B6CF1AF585AB6C8482A8C5398AB1D2DC3CB92E9EA68F
SHA-512:	616B06A6E3B2385E5487C819FC7F595D473B2F14E8CB76EFB894EDEAB3B26D2C9B679A9B275D924BECC37E156C70B0B56126CCFB62C8B23ABBA9DE07BD93D2A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/HdepnBaFj-yarvouFUIlfV4Q9D8.gz.js
Preview:	var __spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u};define("clientinst",["require","exports"],function(n,t){function it(){a=0;u()}function u(){var n,s,t,o;e&&clearTimeout(e);for(n in i)if(i.hasOwnProperty(n)){s=n!=_G.IG?_G.lsUrl.replace(_G.IG,n):_G.lsUrl;for(t in i[n])i[n].hasOwnProperty(t)&&(o=b+s+"&TYPE=Event."+t+"&DATA="+f("[")+i[n][t]+f("]"),ut(o)||(g().src=o));delete i[n]}typeof r!="undefined"&&r.setTimeout&&(e=r.setTimeout(u,w))}function rt(){return _G!==undefined&&_G.EF!==undefined&&_G.EF.logsb!==undefined&&_G.EF.logsb===1}function ut(n){return rt()?ft(n,""):!1}function ft(n,t){var i="sendBeacon",r=!1;if(navigator&&navigator[i])try{navigator[i](n,t);r=!0}catch(u){}return r}var y,d,i,g,o,p;t.__esModule=!0;t.Wrap=t.Log2=t.LogInstrumented=t.Log=t.LogCustomEvent=void 0;var r=n("env"),s=n("event.native"),h=n("e

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	67125
Entropy (8bit):	5.23613773666319
Encrypted:	false
SSDEEP:	768:PfY2/W3m6CHbtHgtBkrel21k4Q8BLBSaJBe7BHyJxBCGnVW4nMO51sEBvkH7BSVq:Y2rA3cnq5QPW4nMETv8jYXmNw6V+oF
MD5:	7A6E7F57E8AA30D249A26C481B6CE82C
SHA1:	9902B8665387415875CE0037E4C656F1153D2C
SHA-256:	BAAFA901C91AFC368F4C5443428A247ABE016AD95843AD74148D4321CC0D34DC
SHA-512:	553F287EAEA2583475A96D4F66685C0505FA3961348413F42996631E0F80FC3FF57389EFA6FD5E862F06CAE7110B818BFEED071DF96495CA9EBFB7BCA6FD6162
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\Lq2ZTcK-ZOpjsEJIXReQZG4mDLg.gz[1].js	
Preview:	var AutoSuggest,__extends,Bing,sa_inst;(function(n){var t;(function(n){var t,i,r,u,f,e;(function(n){n.User="SRCHHPGUSR"})(t=n.CookieNames||(n.CookieNames={})),function(n){n.AutoSuggest="AS"}(i=n.CrumbNames||(n.CrumbNames={})),function(n){n.CursorPosition="cp";n.ConversationId="cvid";n.SuggestionCount="sc";n.PartialQuery="pq";n.SuggestionPosition="sp";n.SuggestionType="qs";n.PreviewPaneSuggestionType="qsc";n.SkipValue="sk";n.PreviewPaneSkipValue="skc";n.Ghosting="ghc";n.Css="css";n.Count="count";n.DataSet="ds";n.SessionId="sid";n.TimeStamp="qt";n.Query="q";n.ImpressionGuid="ig";n.QFQuery="qry";n.BaseQuery="bq";n.FormCode="form";n.HashedMuid="nclid";n.RequestElToken="elvr";n.ElTokenValue="elv";n.AppId="appid";n.History="history";n.NoHistory="nohs";n.ApiTextDecoration="textdecorations";n.ClientId="clientid";n.Market="mkt";n.Scope="scope";n.CountryCode="cc";n.HomeGeographicRegion="hgr";n.SetLang="setlang";n.ZeroInputSerp="zis"}(r=n.QueryParams||(n.QueryParams={})),function(n){n.ImpressionG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\MstqcgNaYngCBavkktAoSE0--po.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	391
Entropy (8bit):	5.184440623275194
Encrypted:	false
SSDEEP:	12:2Qxjl/mLAHPWEaaGRHkj6iLUEkFKgs5qHT:2QC8H+aGRHk+i1kFKgs5qHT
MD5:	55EC2297C0CF262C5FA9332F97C1B77A
SHA1:	92640E3D0A7CBE5D47BC8F0F7CC9362E82489D23
SHA-256:	342C3DD52A8A456F53093671D8D91F7AF5B3299D72D60EDB28E4F506368C6467
SHA-512:	D070B9C415298A0F25234D1D7EAFB8BAE0D709590D3C806FCEAEC6631FDA37DFFCA40F785C86C4655AA075522E804B79A7843C647F1E98D97CCE599336DD9D9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MstqcgNaYngCBavkktAoSE0--po.gz.js
Preview:	(function(){function n(){var n=_ge("id_p"),t,i;n&&(t="",i="",n.dataset?(t=n.dataset.src,i=n.dataset.alt):(t=n.getAttribute("data-src"),i=n.getAttribute("data-alt")),t&&t!=""&&(n.onerror=function(){n.onerror=null;n.src="";n.alt=""},n.onload=function(){n.alt=i},n.src=t)}n()})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NGDGShwgz5vCvyjNFyZiaPlHGCE.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	252
Entropy (8bit):	4.837090729138339
Encrypted:	false
SSDEEP:	6:qbLkyK4hImTzBwhLM1whA+XzFE8KSiQLGPQQgnaqza:IQD2IkzaLMGAMzDBVKY+ia
MD5:	1F62E9FDC6CA43F3FC2C4FA56856F368
SHA1:	75ADD74C4E04DB88023404099B9B4AAEA6437AE7
SHA-256:	E1436445696905DF9E8A225930F37015D0EF7160EB9A723BAFC3F9B798365DF6
SHA-512:	6AADAA42E0D86CAD3A44672A57C37ACBA3CB7F85E5104EB68FA44B845C0ED70B3085AA20A504A37DDEDEA7E847F2D53DB18B6455CDA69FB540847CEA6419CDBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/NGDGShwgz5vCvyjNFyZiaPlHGCE.gz.js
Preview:	var Button;(function(){WireUp.init("button_init",function(n){var t=n.getAttribute("data-appns"),i=n.getAttribute("data-k");sj_be(n,"click",function(){Log.Log("Click","Button","",!1,"AppNS",t,"K",i,"Category","CommonControls")})})})(Button||(Button={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284FD
Malicious:	false
IE Cache URL:	res://ieframe.dll/NewErrorPageTemplate.css
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #000000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\bLULVERLX4vU6bjspboNMw9vl_0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	very short file (no magic)
Category:	downloaded
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:V:V
MD5:	CFCD208495D565EF66E7DFF9F98764DA
SHA1:	B6589FC6AB0DC82CF12099D1C2D40AB994E8410C
SHA-256:	5FECEB66FFC86F38D952786C6D696C79C2DBC239DD4E91B46729D73A27FB57E9
SHA-512:	31BCA02094EB78126A517B206A88C73CFA9EC6F704C7030D18212CACE820F025F00BF0EA68DBF3F3A5436CA63B53BF7BF80AD8D5DE7D8359D0B7FED9DBC3A 99
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/bLULVERLX4vU6bjspboNMw9vl_0.gz.js
Preview:	0

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
IE Cache URL:	res://ieframe.dll/dnserror.htm?ErrorStatus=0x800C0005&DNSError=0
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon-2x[1].ico	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	MS Windows icon resource - 1 icon, 32x32, 32 bits/pixel
Category:	downloaded
Size (bytes):	4286
Entropy (8bit):	3.8046022951415335
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\favicon-2x[1].ico	
SSDEEP:	24:suZOWcCXPRS4QAUs/KBy3TYI42Apvl6wheXpktCH2Yn4KgISQggggFpz1k9PAYHu:HBRh+sCBykteatiBn4KWi1+Ne
MD5:	DA597791BE3B6E732F0BC8B20E38EE62
SHA1:	1125C45D285C360542027D7554A5C442288974DE
SHA-256:	5B2C34B3C4E8DD898B664DBA6C3786E2FF9869EFF55D673AA48361F11325ED07
SHA-512:	D8DC8358727590A1ED74DC70356AEDC0499552C2DC0CD4F7A01853DD85CEB3AEAD5FBDC7C75D7DA36DB6AF2448CE5ABDFF64CEBDCA3533ECAD953C061A9338E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/sa/simg/favicon-2x.ico
Preview:	....(... ...@..... .....N...Sz..R...R...P. ..N..L..H..DG.....R6..U...U...S...R...P...N..L..I..F..B...7.....S6..V...V...U...S ...R...P...N..L..I..F..C...?...z.....O...W...V...V...U...S...R...P...N..L..I..E..C...?...;..{7..q2$.....T..D ..]...S)..p6..J...R...P...N..L..I..E..B..>..;..z7..p2..f,X.....A..O#..N!..N!..N!..P$..q:...P...N..K..I..E..A..=..9..x5..n0..e,...5..... .....Ea.Z,..T$..T$..T

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\gDsOfTXNZVl18jxNDvhXqAdf2tM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1821
Entropy (8bit):	5.098212659804913
Encrypted:	false
SSDEEP:	48:0N3GKBel/r5+8cDYC1YvHIH6ayskysb6NccyskpY3Imqc+DkR:oGKBelzw8fCuoaay5ySSy5q3Mc+4R
MD5:	EC15EB7CBFBFAA68BB1DE04A28C80270
SHA1:	D2570D4CFF3139EA66D15799C9E67211F5A03B20
SHA-256:	810A85F1E705231989251F3EB52DAFF3F0ACEE09C703339C301A7CBD22CF8FE6
SHA-512:	077446A676E47447CB771A119CD0EC2EC168E65FED4579E663866D2846F51E93B47367518EB9D79E04EACE139CDFF043E1E28D64559412B4770388B2FEF96A21
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/gDsOfTXNZVl18jxNDvhXqAdf2tM.gz.js
Preview:	(function(){function b(e){var l=e[1],s=l&&_ge(l.vid);s&&(h=_ge("bnp.nid."+f),i=n.getAttribute("data-overlay")==="true"?!0:!1,c=n.getAttribute("data-setscroll")==="true"?!0:!1,k(),ClassUtil.removeClass(h,y),s.style.display="block",c&&d(),sj_evt.fire("bnp.notif.shown",s),i?nt():sj_evt.fire("McpDismissed"),u=_ge(w),t=_ge(v),t.focus(),r=_ge(p),u&&sj_be(u,o,tt),t&&sj_be(t,o,g))}var v="bnp_btn_accept",o="click",y="b_hide",p="cookie_preference",w="bnp_btn_preference",r,u,t,n=_ge("bnp_cookie_banner"),s=_ge("b_footer"),f=_w.bnp.pb_sttc.id,h,e,i,c,k=function(){var t=n&&n.getAttribute("data-position"),i=_ge("bnp_container");i&&t&&t.toLocaleLowerCase()=="top"&&(i.style.top=t+"px",i.style.bottom="auto")},d=function(){var i=_ge("bnp_container"),r=_ge("bnp_action_container"),n=_ge("bnp_content_desc"),u=_ge("bnp_title_container"),t;i&&r&&n&&u&&(t=i.offsetHeight-(r.offsetHeight+u.offsetHeight+130),n.style.maxHeight=t+"px",t<280&&(n.style.marginRight="-10px"))},g=function(t){ManagedCookiePreferenceActio

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\lK_FmcR4naKX9hplwfe9ify1hf4.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	125734
Entropy (8bit):	5.670169400028476
Encrypted:	false
SSDEEP:	1536:ppkCMu1Rv0SuDHT4kfr5IRnO8E9FqJCnq1EoAXycCroA0wT8aHs3:3Mu1Rv0SvNmeGq1ENXdTAVM
MD5:	C24FE194A488B12CCE5B3858D12C2C3D
SHA1:	E55B3E549CA42D614BEE0C4538F9EDA6C89DE00D
SHA-256:	45A1BD96D9A1BB1F03191C2F062FDC5369542864C4777A67623811BE6463D4D6
SHA-512:	4F1C02C2FE716DBEAF061DC9476AD35E33F5C808FD3D79D0ADBECED81B65A02225F7356DBCB10A7232BDD7D02BC0C908F17BB61B058FF5FB99747202522B543
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/lK_FmcR4naKX9hplwfe9ify1hf4.gz.js
Preview:	var __assign=this&&this.__assign||function(){return __assign=Object.assign||function(n){for(var t,r,i=1,u=arguments.length;i<u;i++){t=arguments[i];for(r in t)Object.prototype.hasOwnProperty.call(t,r)&&(n[r]=t[r])}return n},__assign.apply(this,arguments)},__rest=this&&this.__rest||function(n,t){var u={},r;for(var i in n)Object.prototype.hasOwnProperty.call(n,i)&&t.indexOf(i)<0&&(u[i]=n[i]);if(n!=null&&typeof Object.getOwnPropertySymbols=="function")for(r=0,i=Object.getOwnPropertySymbols(n);r<i.length;r++)t.indexOf(i[r])<0&&Object.prototype.propertyIsEnumerable.call(n,i[r])&&(u[i[r]]=n[i[r]]);return u},__spreadArrays=this&&this.__spreadArrays||function(){for(var i=0,n=0,r=arguments.length;n<r;n++)i+=arguments[n].length;for(var u=Array(i),f=0,n=0;n<r;n++)for(var e=arguments[n],t=0,o=e.length;t<o;t++,f++)u[f]=e[t];return u},__awaiter=this&&this.__awaiter||function(n,t,i,r){function u(n){return n instanceof i?n:new i(function(t){t(n)})}return new(i||(i=Promise))(function(i,f){function o(n){

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sbi[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	46137
Entropy (8bit):	5.492718429280291
Encrypted:	false
SSDEEP:	768:WkuL2ym/YIZE2u1U5l7Ez+YIdQFSO4FWCPPZPzATfZjFwummSczZxG3IuO7JUDWB:plB1FWCpPwkNijuSjyir
MD5:	8147A3C6CCDAD2147CA32BA6DB54E40A

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\sbi[1].htm	
SHA1:	3257CCC8CED1107ACBE3697B61F1C5ED3A86A4E6
SHA-256:	E783F26B771F68588FF468DE04C50E6A3E7BC4A11FEBDB52A17511E9DFE91297
SHA-512:	005695CB7F9FBB397109F11FDD375F23D5C678C7F26036E3937C916F75C96857F6A7C1B10D5820588461479A14B69026A3277389E5C02D09359D5A2BD9CF3C67
Malicious:	false
IE Cache URL:	http://https://www.bing.com/images/sbi?mmasync=1&ptn=Homepage&IID=SBI&IG=6D87EF62E1634929B1A2A3B71ACC6B63&form=REDIRERR
Preview:	<style type="text/css">#sbiarea,#sbicom{display:none}.hassbi #sbiarea{display:inline-block}#sbiarea{margin:0 0 0 18px}.sbox #sb_form #sbiarea{margin:0}#sb_sbi{display:inline-block;cursor:pointer}img#sbi_b{vertical-align:-2px;height:20px;width:20px}#detailPage #detailheader img#sbi_b,.blue2#miniheader img#sbi_b,.sbox img#sbi_b{vertical-align:-3px}.blue2#miniheader img#sbi_b{vertical-align:-1px}#sbi_b.grayscaled{filter:grayscale(1) brightness(1.4);-webkit-filter:grayscale(1) brightness(1.4)}#sbi_b.grayscaled:hover{filter:grayscale(1) brightness(1);-webkit-filter:grayscale(1) brightness(1)}#sb_sbip[shdlg] #sbi_b{filter:grayscale(0);-webkit-filter:grayscale(0)}#sb_sbip .rms_iac{display:inline-block}#sb_sbip:not(.disableTooltip):hover::before,#sb_sbip.shtip:not(.disableTooltip)::before,#sb_sbip[vptest]::before{bottom:-27px;left:10px;z-index:6}#sb_sbip:not(.disableTooltip):hover::after,#sb_sbip.shtip:not(.disableTooltip)::after,#sb_sbip[vptest]::after{top:40px;left:10px;z-index:4}#hp_contain

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\test[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.373593025747649
Encrypted:	false
SSDEEP:	3:UMs1TE5LH0cHrJU4YCf:U37cVUof
MD5:	E82D9BD501B46DF5CB2B650AF9E1B126
SHA1:	0FE6876226E88D8104ED51CB6329EB172BBA8D68
SHA-256:	C2BA8FCCFC980BCC8FC24E7A41BFCFEE88CCA9331C8D4D62890D7DFAB4A12226
SHA-512:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662 4
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3889
Entropy (8bit):	7.890192281255403
Encrypted:	false
SSDEEP:	96:5PEjfzwzrOzplwYpimMhIO+Mtm/dZ7a/ve5Suu86PRg2CY/:5P9zizploVKOT0lZO/vCuZPRgc
MD5:	C42031184BC6E5683A2647F391637A4C
SHA1:	45202C0BD8BC0B7835B375DEB9DA76C5658B2F17
SHA-256:	2FCC6397F43A3884B2D1BA97B82A6F269E8B1C9EA8CCB6B072C6124DBD2879D8
SHA-512:	89C84780EE00A098CF9C5839E074FA2B209920E9E9366D7906E30CD017F8350B5D1F72AF67A36A34CACEAF48FD855CDA410E52BA57756BF9D274DFA5E42DC86 F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flkPJ.img&ehk=ixnfMu%2bvNEGorqMeHZVbV%2bYB9uGjNgR%2bqRDm083wmkQ%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..T2X. .+....w*..5zZN..U...x.6.q....?y..sE).....))k.....Q@...4f.....J..Q...Ob..$u:<...._....>:sM...=n.7On;W..i.}\..a.|...R0H..."&h.!..b..m)..D.-..P..Y....dW-.}.....[OSn..n1..q.;.Y".....^e.i..3...I.wKIK^....$0.q .%...2..]?..\....X.1...U.M.i...../.S.....R...<.g3.....~c..7.u.:p\G*.w.....S'x...Q\..I..RBA...z.5.]....Y.,I...L-.t..-.....w.#..@..W.O.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4103
Entropy (8bit):	7.905624591549082
Encrypted:	false
SSDEEP:	96:pPE7azjJGnUjIWZ3fWfX6c11tzgyuBDgYNgdZ/z:pPQkJHsccXV11tzgDBDgYaz
MD5:	D79048C62D1919EBD68359F962DE7D0C
SHA1:	56CA765E294DD844FCD7D56339AC81647DEF4D8E
SHA-256:	92B97018B5A41B256E26BDCB5764E3076A44FF3B2DD3C89FC3E1C20A024EA559
SHA-512:	1F91EC0DF06E58899F1EC644F654C1CE069DDFC6DFB6B8F545B6C66D71867797D420D899D7152EE99729B86888589E3FBED27CE56277B3B2DB3C4FFD829AEA B
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\th[2].jpg	
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fiIcx.img&ehk=u4rkWZofWQoQJ11NQ%2fu8JYLsufAv%2fujiPAfuy3supnc%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..H..C...7CVWED..1a..-.....<R].O....(..6...w..T.R..mS..6.%.@b.....Uf...C.%.o..T....M..N...]lw4P..<[.I.3).)$... d{sM..g.V..S...~..W...khU}H..B.)\.!..&'M.F..f.:.'#.tFI..b2)P..U.`..m;.%".....AKE..))i. .....bo.j.....A..4.,...<.K4.$..pOz.....-:..... .'".....v..T.\g.O.=MQ.E..fV..|.l/....U.....ZRB..Q.~..V.....K.o(r.E.....t$.....P.<H..3.~.....{.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3742
Entropy (8bit):	7.867632755628144
Encrypted:	false
SSDEEP:	48:pyYcuERAFyZuPbJdd/1D9uU8lPjsEO/pjKnTLdyW+Tm8bV8SANcggbCPdXBUAxaB:pPECyZ6DEU8SEOOLuSMHBggupBBYBzf
MD5:	76A08CC374F645ADFD2D574AEA9E1F67
SHA1:	EF6301792289F45E1914290BD3901BE5C3C08ED7
SHA-256:	6D4A8E2E63961DF63F503AC5A323D9FAD4F738E8720BD98C9A302794CB62847C
SHA-512:	19AADD5296DEA0C5F8D8165911C2ABF00A7BED8E98C7090448664715E99559D92DE6D6196EBE8D7A546A33704BD36A596A85F847DFFBAA3C2BC6E818707F31EA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjVGq.img&ehk=CUJArgAlYOIs%2fdufnie%2fHn0v5FuoJklhhKQfEtkFJ8l%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..r).r)..4..T..(.....'....m.m./....cjd..$D ..v...qj.....}+SN.}.p.Y.F..*[CQfI.Y..1.....>.....!..8..2@.U....Yn.9..F..[....0.o.#)R.@....z3..o..$..3.1....{..%OQ...S..!$}.{}k.....y....-Y.KF)qV .!....G....|..K.@.R.J.3.-S(..W..~*.....+CD...lZ..(d...P.b.?6.P3....Q.j7.}.4t.....8.....X.YC5.ae.....V"....n.0'..i.`.....a.v (fo....S....S\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5639
Entropy (8bit):	7.924649163999842
Encrypted:	false
SSDEEP:	96:pPECr5OAvlqY/K2/QGjfn7l0xXDUduR+Ksxd18Up0FlXDmR6vhOjUEbDdl:pPnOAvlh/KXGf7LxXDUd2kd6XbbOgEbT
MD5:	CB467408920B249304F096825FAD3555
SHA1:	34B1FB66BB1993D6F421D03E60571B2D6B8BD82B
SHA-256:	6244F0B65FD5FDB55035289E22AE746FDA4FB8A73FA5099AC1765FE40EBF15F3
SHA-512:	66499CCD7720806D8D469F36F1BA68B8654C4113F6EC8952C30B0B7A5456CE7B942E535389026532315054070O3DF5D6EC55402114F39FEB6EE135B6B803BC60
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk8uF.img&ehk=3yVhb5eiLjVCrnzpfMt8vNf6P4rYdQzaUR6b8msklWU%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?....I.5Zo1..{V}.W..3.w...@..>..^...8I.U..b..k.....<..1J".[..>..."f...`.U...$V..C...ZfzF...V.R...-....r=G4.....LD....[.D\..*....w.h..R1&..z...'.1.#..i.w..{PH*p.@/..B..&..9..{]].0..{.RT...>.....0.Y.Q...3[).....q.....>.}OX...Y..:....r.@k.@..Fy0.<....i.j.....t.9\gp..j.v...~.+..#...&q.5zH.JYW.cry.,...9o.3..r...G .z..j.'..{X.-t..(S8.;...Q....N.<...._....'..Z.:.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\v[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, max speed, from TOPS/20
Category:	dropped
Size (bytes):	372
Entropy (8bit):	7.411391890964964
Encrypted:	false
SSDEEP:	6:XtOyZEx1sRE+oYR5ftkShaO4Te6bb2kvDL87dkR4/5RfsMJlWxYYb3xWTfl0yggk:XYYEjsXxfZF4TZbrvnqdY4EMJlAz3ONU
MD5:	371A69B9C7D1E3610507DA49FB5FBA08
SHA1:	F9471C418625643A201195080154C6B3F013A16A
SHA-256:	FA1AF38BC482FBC80EC0DC9490C4B122375A28F3CF20F743430F40A4772EF08F
SHA-512:	6B5C0E501763F07EFD4473D28479F630360C76A7AC02A5E2EA8CDE2DFCA6F2D0AC16866B16C49B93682F8D581BEB500522423B6E839832913F176A17879A2202
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\0W10PBUV\v[1].htm	
Preview:	.....T.MS.@.....}.]......lB.../..+....b...:u}.9=....l*..m.JU.{.nE..us.9.?F..H...>?...i...(..Nl&.R...5@.....u...i.C@...wk@.y...2+AvX[_E.,..0...#z....Dk.c...c. .....R.*..m.1.....g.K. .N....4...(....L6_...../.H...6.f....Q..g/.(4b...fw5.#'...el....k8/.=..Q<...A..0.%8N....>...C..~..U.O.K^..t"/.....Z..W.N|.A.L_w.....].Rt.....$.....~...}.....Jw....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\9[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	gzip compressed data, max speed, from TOPS/20
Category:	dropped
Size (bytes):	365
Entropy (8bit):	7.333764238743036
Encrypted:	false
SSDEEP:	6:XtCEUWoeY+gODzpr+eg5A7ok3pxzkllNpihZqfU2sGwjvKSc6moJR2AFcWMhT+:XE3eYwFr+ega8W4NwhzFGwbKSvHJR2A3
MD5:	D9E38431D1D450B91858488E1A134326
SHA1:	319D5DCA045A9C4C4E95930D07E3A7E4FF7CFF94
SHA-256:	7F51510C33515D9FCAD21DB4A59818340E84D49563EE2711D2EC07239B7033BA
SHA-512:	3E3F4066E82E4DDFA9FB81F037460EFE6E9F5EA1666F1B04A72B24FE9EED7608B467FB01608ED33410E1ED9E93522727FE6B6F2C3D3E46D3F795DE6247A66152
Malicious:	false
Preview:	.....T.AS.@.@.....Lj.I...mLA.....A.....;.G.,..pF...\.L_EG..^)....2.W#..~{C8.....5K'}.....m.A.W. ....(DYP.%wRg.>v.1...).L.._f.S.9`+....Bq\..... ^.J.....~..3.r..5..L.B\o< .y...@f.l....1dI..../.u.l.{..6...ly./....;.....;S.....<.....P.[.m.(.....H.6....R.m;Q.hyz.Y.g....^Gc.....-s<...jY.pl....u.jF.....Ka..-.7.....b.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Jl2vUSlElqWjk-99MuYp4W74zvQ[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image
Category:	downloaded
Size (bytes):	1529
Entropy (8bit):	4.135964697042234
Encrypted:	false
SSDEEP:	24:tVvnjuJOeUsc4wg5a2/gt+lm/3HljKR99U1TrD3ptYZ7GDlh6mI0jeI4dIwDq8rz:rn1edcjg5pm/lKRXU1TrD5tJf6mzjidJ
MD5:	6D8EF11CB1C03B39D9ED4E4C9A2190B9
SHA1:	265DAF51294422A5A393EF7D32E629E16EF8CEF4
SHA-256:	D72BEAE30A6B2B36C3E03847CE4EA04211D7373D4066FF937A7A05DF4E0C3DB6
SHA-512:	C8820BDF2FC34CCFF7018A1C1E3E74ED1FE0B287926050F9B6BA59C08DCC216E8732F862AB0BF086BC05275C51E6F81132AFA60F6D50A19585642BC906DCDD 2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Jl2vUSlElqWjk-99MuYp4W74zvQ.svg
Preview:	<svg width="16" height="16" viewBox="0 0 16 16" fill="none" xmlns="http://www.w3.org/2000/svg">..<path d="M8 0C6.41775 0 4.87103 0.469192 3.55544 1.34 824C2.23985 2.22729 1.21447 3.47672 0.608967 4.93853C0.00346629 6.40034 -0.15496 8.00887 0.153721 9.56072C0.462403 11.1126 1.22433 12.538 2.34315 13.6 569C3.46197 14.7757 4.88743 15.5376 6.43928 15.8463C7.99113 16.155 9.59966 15.9965 11.0615 15.391C12.5233 14.7855 13.7727 13.7602 14.6518 12.4446C15.5 308 11.129 16 9.58225 16 8C16 5.87827 15.1571 3.84344 13.6569 2.34315C12.1566 0.842854 10.1217 0 8 0V0Z" fill="white"/>..<path d="M3.72395 9.60957L5.72394 11.6096C5.97398 11.8595 6.31306 12 6.66661 12C7.02016 12 7.35924 11.8595 7.60928 11.6096L12.2759 6.9429C12.4033 6.81991 12.5049 6.67278 12.5747 6 .51011C12.6446 6.34744 12.6814 6.17248 12.6829 5.99544C12.6845 5.8184 12.6507 5.64283 12.5837 5.47897C12.5167 5.3151 12.4177 5.16623 12.2925 5.04104C1 2.1673 4.91585 12.0184 4.81685 11.8545 4.74981C11.6907 4.68277 11.5151 4.64903 11.3381 4.65057C11.16

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\NewErrorPageTemplate[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1612
Entropy (8bit):	4.869554560514657
Encrypted:	false
SSDEEP:	24:5Y0bQ573pHpACtUZtJD0lFBopZleqw87xTe4D8FaFJ/Doz9AtjJgbCzg:5m73jcJqQep89TEw7Uxkk
MD5:	DFEABDE84792228093A5A270352395B6
SHA1:	E41258C9576721025926326F76063C2305586F76
SHA-256:	77B138AB5D0A90FF04648C26ADDD5E414CC178165E3B54A4CB3739DA0F58E075
SHA-512:	E256F603E67335151BB709294749794E2E3085F4063C623461A0B3DECBCCA8E620807B707EC9BCBE36DCD7D639C55753DA0495BE85B4AE5FB6BFC52AB4B284F D
Malicious:	false
Preview:	.body..{.. background-repeat: repeat-x;.. background-color: white;.. font-family: "Segoe UI", "verdana", "arial";.. margin: 0em;.. color: #1f1f1f;..}.....mainContent..{.. margin-top:80px;.. width: 700px;.. margin-left: 120px;.. margin-right: 120px;..}.....title..{.. color: #54b0f7;.. font-size: 36px;.. font-weight: 300;.. line-height: 40px;.. margin-bottom: 24px;.. font-family: "Segoe UI", "verdana";.. position: relative;..}.....errorExplanation..{.. color: #000000;.. font-size: 12pt;.. font-family: "Segoe UI", "verdana", "arial";.. text-decoration: none;..}.....taskSection..{.. margin-top: 20px;.. margin-bottom: 28px;.. position: relative; ..}.....tasks..{.. color: #00 0000;.. font-family: "Segoe UI", "verdana";.. font-weight:200;.. font-size: 12pt;..}....li..{.. margin-top: 8px;..}.....diagnoseButton..{.. outline: none;.. font-size: 9pt; ..}.....launchInternetOptionsButton..{.. outline: none;

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz[1].js	
Category:	downloaded
Size (bytes):	930
Entropy (8bit):	5.191402456846154
Encrypted:	false
SSDEEP:	24:GFUFqJYYmaLOTCE20aOtZP9F3a6MakIq+IvyUJ9sq5aOB:BWOWEZP9U6MHEvyUJ9s6
MD5:	73BFB9BB67A7271E257A4547007469A5
SHA1:	28F7B820679A99318E0DC596A54480D6AD5C3661
SHA-256:	A22BB5BD48C4C578C6BC4FDC4B8FF18F9162848F14E05AE283EC848B08EC8C15
SHA-512:	432142851A492C7635B764AC5293B6EFC943624FBD2FEA5D0F2D8900208B5F6233F5563B7CC08F314E29889B2628F2983554847008 16A3679F6A3315E63581F0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/PA3TC2iNXZkiG2C3IJp5VAvC_yY.gz.js
Preview:	var ShareDialog;(function(n){function i(){t("bootstrap",arguments)}function r(){t("show",arguments)}function u(){t("showError",arguments)}function t(n,t){for(var r=["shdl gapi",n],i=0;i<t.length;i++)r.push(t[i]);sj_evt.fire.apply(null,r)}n.bootstrap=i;n.show=r;n.showError=u})(ShareDialog||(ShareDialog={})),function(n){function i(){t==0&&u( )}function r(){sj_evt.unbind("shdlgapi",i)}function u(){t=1;var n=ShareDialogConfig.shareDialogUrl+"&IG="+_G.IG;n=e(n,["uncrunched","testhooks"]);sj_ajax(n,{callback:func tion(n,i){n?(t=2,i.appendTo(_d.body),r(),f()):t=3},timeout:0})}function f(){var n="rms";_w[n]&_w[n].start()}function e(n,t){var i,r,u;for(r in t)u=new RegExp("[?&]"+r+"=[^? &#]*","i"),(i=location.href.match(u))&&i[0]&&(n+="&"+i[0].substring(1));return n}function o(){n.inited=0}function s(){n.inited||(n.inited=1,sj_evt.bind("shdlgapi",i,!0),sj_evt .bind("ajax.unload",o,!1))}var t=0;s()}(ShareDialog||(ShareDialog={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\Passport[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	329
Entropy (8bit):	5.086971439676268
Encrypted:	false
SSDEEP:	6:qzxUe3X965+zAqEFtTNfYEAn4TXQ3SOFCL0H4WZhCroOI:kxFkXq6tTRYEVTAx4IHH7CroOI
MD5:	7B7D5DA1B057EB0D5A58C2585E80BACA
SHA1:	29714CD8C570E321C1C1C991E77ACE3945312AC6
SHA-256:	023CD9B7315636BE1BE24DC78144554B0E76777BD476ED581378172DE9B12A05
SHA-512:	1A4E36E3124968166579C04D05A1325242E1DFE20DF4C804081487A019B88395A679A439525488F78B73334C5B0BD38D61E24F8E23F2F8274C6BAC323291CEE8
Malicious:	false
Preview:	<html><head><title>Bing</title></head><body>Loading...<script type="application/x-javascript">//<![CDATA[.var _w = window; var o = _w.opener; var mainWindow; (m ainWindow = o) || (mainWindow = _w.parent); if (mainWindow) {mainWindow.sj_evt && mainWindow.sj_evt.fire("wl:cancel"); };if (o) _w.close();;.// </script></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\dnserror[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	2997
Entropy (8bit):	4.4885437940628465
Encrypted:	false
SSDEEP:	48:u7u5V4VyhhV2lFUW29vj0RkpNc7KpAP8Rra:vlIJ6G7Ao8Ra
MD5:	2DC61EB461DA1436F5D22BCE51425660
SHA1:	E1B79BCAB0F073868079D807FAEC669596DC46C1
SHA-256:	ACDEB4966289B6CE46ECC879531F85E9C6F94B718AAB521D38E2E00F7F7F7993
SHA-512:	A88BECB4FBDDC5AFC55E4DC0135AF714A3EEC4A63810AE5A989F2CECB824A686165D3CEDB8CBD8F35C7E5B9F4136C29DEA32736AABB451FE8088B978B493 AC6D
Malicious:	false
Preview:	.<!DOCTYPE HTML>..<html>.. <head>.. <link rel="stylesheet" type="text/css" href="NewErrorPageTemplate.css" >.. <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">.. <title>Can’t reach this page</title>.. <script src="errorPageStrings.js" language="javascript" type="text/javascript">.. </script>.. <script src="httpErrorPagesScripts.js" language="javascript" type="text/javascript">.. </script>.. </head>.... <body onLoad="getInfo(); initMo reInfo('infoBlockID');">.. .. Can’t reach this page .. .. <ul id="cantDisplayTasks" class="tasks">.. <li id="task1-1">Make sure the web address is correct .. <li id="task1-2">Search for this site on Bing ..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\down[1]	
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44
Malicious:	false
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....I..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\errorPageStrings[2]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
IE Cache URL:	res://ieframe.dll/errorPageStrings.js
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts ";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet conn ection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the web site you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\model[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	16168
Entropy (8bit):	5.527579595880806
Encrypted:	false
SSDEEP:	384:HUQyIePm3yt9YYQ5bV5u5hOuKsVMhu3kx0m4iDewY/rfrEraIO1uYPW:0yZ3yjYY85uTOuKsV2u3kx0m4iDewY/i
MD5:	B12C190DFA30C8EF3CACFB2304F8A6BB
SHA1:	4485BA9BCEC741F844120DA43AD4C67EED5EFF0F
SHA-256:	E18575EBB4698CD7418A52E923B8815AA1B288FB160F12A9B8DFE69C816FCA67
SHA-512:	0BE8328FD43826911A8BDD74E85C052F47EA08AF97F36C5C8296648B037C60CFEDA186F81A08C1620728FD50F5D3F36C634CCD2D943C41BEE3DDF3F69515B73
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/model?form=REDIRERR
Preview:	{"ClientSettings":{"Pn":{"Cn":1,"St":0,"Qs":0,"Prod":"P"},"Sc":{"Cn":1,"St":0,"Qs":0,"Prod":"H"},"Qz":{"Cn":1,"St":0,"Qs":0,"Prod":"T"},"Ap":true,"Mute":true,"Lad":"2021-04-06T00:00:00Z","Iotd":0,"Dft":null,"Mvs":0,"Flt":0,"Imp":2},"MediaContents":[{"ImageContent":{"Description":"The first modern Olympic Games were held 125 years ago in A thens in 1896 . 1,500 years after they were banned by the Roman Emperor. The 1896 Games were held in the Panathenaic Stadium, in the shadow of the Acropolis of Athens, shown here. They included athletes from 14 countries, with the largest delegations from Greece, Germany, France and Great Britain. The 43 events included a marathon, tennis, cycling, fencing, shooting, Greco-Roman wrestling and swimming. And while some things haven't changed over the years, some were different back then. Swimmers were taken out to sea by boat for the longer races and had to swim back to shore. Winners were given a silver medal (copper for second place), as well as an o

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\msnpopularnow[1].json	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	10501
Entropy (8bit):	5.51784121777492
Encrypted:	false
SSDEEP:	192:LUuCIrvL8IgVoZvJZvtctCQwyltHEZdrXgsqBv6SHGjHHAHaBaZvkr1qPUaDQAby:LBCOVmUzaBDePrwsUS/k6Ba52qPJQZEW
MD5:	FC690FA0CC46C5CF583DFBBE141E5A58
SHA1:	E7CCC631BEAE8AC7DC42B1A8259BC752E4938D6F
SHA-256:	8498F9C879FE298FB470D1DB0811F56401425DFBE2388B282C7935FA1E4AC854
SHA-512:	FB1FA394B996687B25D6B05DDC9C77D78538CF281B18E4FD4E797229D68B3C2C692F561AD07B60345078366B2BA27CBFA08B2D2717095D1FBBD0D7159B55959
Malicious:	false
IE Cache URL:	http://https://www.bing.com/hp/api/v1/msnpopularnow?&format=json&ecount=20&efirst=0&&form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\msnpopularnow[1].json	
Preview:	{"title":"","data":[{"typeName":"Msn","items":[{"url":"https://www.msn.com/de-ch/news/other/der-westen-muss-mit-sanktionen-drohen-die-wehtun/ar-BB1flkV9?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flnql.img&ehk=e56b2FA%2fdQ8S1%2bJCLPLA5GewBcl71RQ%2fTmEAxvevKks%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"BZ BERNER ZEITUNG","longTitle":"Der Westen muss mit Sanktionen drohen, die wehtun","accessibilityTitle":"","subtext":"","isRecommendedNews":false},{"url":"https://www.msn.com/de-ch/finanzen/top-stories/staatliche-regulierung-allianz-gegen-big-tech-druck-auf-facebook-und-google-w.chst/ar-BB1fkLCT?ocid=BingHPC","imageUrl":"/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0","shortTitle":"Handelsblatt","longTitle":"Staatliche Regulierung: Allianz gegen Big Tech: Druck auf Facebo.","accessibilityTitle":"","

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1567
Entropy (8bit):	5.248121948925214
Encrypted:	false
SSDEEP:	48:KyskFELvJnSYVtXpQyL93NzpGaQJWA6vrIhf7:KybivJnSE5aU93HGaQJWAilh
MD5:	F9D8B007B765D2D1D4A09779E792FE62
SHA1:	C2CBDA98252249E9E1114D1D48679B493CBFA52D
SHA-256:	9400DF53D61861DF8BCD0F53134DF500D58C02B61E65691F39F82659E780F403
SHA-512:	07032D7D9A55D3EA91F0C34C9CD504700095ED8A47E27269D2DDF5360E4CAC9D0FAD1E6BBFC40B79A3BF89AA00C39683388F690BB5196B40E5D662627A2C49A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/n8-O_KIRNSMPFWQWrGjn0BRH6SM.gz.js
Preview:	var wln=wln||"",Identity;(function(n){function i(n){n.style.display="none";n.setAttribute("aria-hidden","true")}function r(n){n.style.display="inline-block";n.setAttribute("aria-hidden","false")}var u,t;n&&n.sglid&&sj_be&&sj_cook&&sj_evt&&_d&&typeof _d.querySelectorAll!="undefined"&&(u=function(n){var i=n.getAttribute("data-a"),t=n.getAttribute("data-p");i==="false"&&t!=null&&sj_be(n,"click",function(){sj_cook.set("SRCHUSR","POEX",t,!0,"/")})},sj_evt.bind("identityHeaderShown",function(){var n=!1;sj_be(_ge("id_l"),"click",function(){var i,t;if(!n){for(i=_d.querySelectorAll(".b_imi"),t=0;t<i.length;t++)u(i[t]);n=!0}})},!0));sj_evt&&n&&(t=function(t){var h;if(t==null||t.idp!=="orgid"||(h=n.wlProfile(),h==null||h.name==null||t.name!=null)){var e=_ge("id_n"),u=_ge("id_p"),o=_ge("id_s"),s=_ge("id_a"),f=t?t.displayName:wln,c=t?t.img:null,l=t?t.idp:null,a=t?t.cid:null;e&&s&&(a||f)?(u&&c&&(u.title=f,u.src=c,r(u)),f.length>10&&(f=f.substring(0,10).replace(/\s+$/,"")+"."),e.textContent=f,e.inn

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	226
Entropy (8bit):	4.923112772413901
Encrypted:	false
SSDEEP:	6:2LGfGIEW65JcYCgfkF2/WHRMB58IIR/QxbM76Bhl:2RWIyYCwk4/EMB5ZccbM+B/
MD5:	A5363C37B617D36DFD6D25BFB89CA56B
SHA1:	31682AFCE628850B8CB31FAA8E9C4C5EC9EBB957
SHA-256:	8B4D85985E62C264C03C88B31E68DBABDCC9BD42F40032A43800902261FF373F
SHA-512:	E70F996B09E9FA94BA32F83B7AA348DC3A912146F21F9F7A7B5DEEA0F68CF81723AB4FEDF1BA12B46AA4591758339F752A4EBA11539BEB16E0E34AD7EC946763
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/ozS3T0fsBUPZy4zlY0UX_e0TUwY.gz.js
Preview:	(function(n,t,i){if(t){var r=!1,f=function(){r||(r=!0,typeof wlc!="undefined"&&wlc(sj_evt,sj_cook.set,wlc_t))},u=function(){setTimeout(f,t)};n.bind("onP1",function(){i?n.bind("aad:signedout",u):u()},1)}})(sj_evt,wlc_d,wlc_wfa)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sbi[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	46137
Entropy (8bit):	5.492718429280291
Encrypted:	false
SSDEEP:	768:WkuL2ym/YIZE2u1U5l7Ez+YIdQFSO4FWCPPZPzATfZjFwummSczZxG3luO7JUDWB:plB1FWCpPwkNijuSjyir
MD5:	8147A3C6CCDAD2147CA32BA6DB54E40A
SHA1:	3257CCC8CED1107ACBE3697B61F1C5ED3A86A4E6
SHA-256:	E783F26B771F68588FF468DE04C50E6A3E7BC4A11FEBDB52A17511E9DFE91297
SHA-512:	005695CB7F9FBB397109F11FDD375F23D5C678C7F26036E3937C916F75C96857F6A7C1B10D5820588461479A14B69026A3277389E5C02D09359D5A2BD9CF3C67
Malicious:	false
IE Cache URL:	http://https://www.bing.com/images/sbi?mmasync=1&ptn=Homepage&IID=SBI&IG=AC882D833DB048C591AAA8C43AC284DE&form=REDIRERR

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\sbi[1].htm	
Preview:	<style type="text/css">#sbiarea,#sbicom{display:none}.hassbi #sbiarea{display:inline-block}#sbiarea{margin:0 0 0 18px}.sbox #sb_form #sbiarea{margin:0}#sb_sbi{display:inline-block;cursor:pointer}img#sbi_b{vertical-align:-2px;height:20px;width:20px}#detailPage #detailheader img#sbi_b,.blue2#miniheader img#sbi_b,.sbox img#sbi_b{vertical-align:-3px}.blue2#miniheader img#sbi_b{vertical-align:-1px}#sbi_b.grayscaled{filter:grayscale(1) brightness(1.4);-webkit-filter:grayscale(1) brightness(1.4)}#sbi_b.grayscaled:hover{filter:grayscale(1) brightness(1);-webkit-filter:grayscale(1) brightness(1)}#sb_sbip[shdlg] #sbi_b{filter:grayscale(0);-webkit-filter:grayscale(0)}#sb_sbip .rms_iac{display:inline-block}#sb_sbip:not(.disableTooltip):hover::before,#sb_sbip.shtip:not(.disableTooltip)::before,#sb_sbip[vptest]::before{bottom:-27px;left:10px;z-index:6}#sb_sbip:not(.disableTooltip):hover::after,#sb_sbip.shtip:not(.disableTooltip)::after,#sb_sbip[vptest]::after{top:40px;left:10px;z-index:4}#hp_contain

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\svl82uPNFRD54V4bMLaeahXQXBI.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	425
Entropy (8bit):	4.963129739598361
Encrypted:	false
SSDEEP:	12:2gXsmzwKN0yApFkRLNF1Jfa1VTWPMg9pIGywV:2gX9zwKN0yAqr1Jfa1V059V
MD5:	016ECFDB34031F881FA5E34DFBD0B7A1
SHA1:	16D3BA1049939D00AE47AAD053993B4762D9B102
SHA-256:	08021ED3BCA5532304B597E636BEB939FF7BAA6D08DCA4E94C0DDE1FDF940389
SHA-512:	D61045D1F07ED241626B8233D388F5E1AD54DBE224871E1CE872ECFD0E29F05A21F0EA02FFDE688FACB134DD969533615493BD35EBA4D5E755840C30A687EE0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/svl82uPNFRD54V4bMLaeahXQXBI.gz.js
Preview:	(function(n){function f(){u(sj_be,r)}function r(i){return i&&n.enqueue(t,i),!0}function e(){u(sj_ue,r)}function u(n,t){for(var u,r=0;r<i.length;r++)u=i[r],n(u==="resize"?window:document,window.navigator.pointerEnabled?u.replace("mouse","pointer"):u,t,!1)}var t="EVT",i=["click","mousedown","mouseup","touchstart","touchend","mousemove","touchmove","scroll","keydown","resize"];n.wireup(t,{load:f,compute:null,unload:e})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\test[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	4.373593025747649
Encrypted:	false
SSDEEP:	3:UMs1TE5LH0cHrJU4YCf:U37cVUof
MD5:	E82D9BD501B46DF5CB2B650AF9E1B126
SHA1:	0FE6876226E88D8104ED51CB6329EB172BBA8D68
SHA-256:	C2BA8FCCFC980BCC8FC24E7A41BFCFEE88CCA9331C8D4D62890D7DFAB4A12226
SHA-512:	D3715E6A3C9012F2D8E1269E5C4B3E2F77FD2CD8E793AD39E51F1E1BE30F0818DDD01FAF3708EF789FDF347B92C6477C10A1155DEC582FF68185CBFD41C662
Malicious:	false
Preview:	IPv6Tests.TestIPv6Response('{"type": "4"}');

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 0x0, segment length 16, baseline, precision 8, 1920x1080, frames 3
Category:	downloaded
Size (bytes):	344983
Entropy (8bit):	7.987666031914428
Encrypted:	false
SSDEEP:	6144:uhr6bFSzjuZdOJGR0u6FY7Kq1u9ktnbQ9uJ4g2FUXoIQc1tYJsDr0j:AwFEjSOJbuYphkZQ9uJX22TQc1qJwa
MD5:	DDCE5ED235CCBFFDA3F3735F75F80C0F
SHA1:	F266C24FA6F01459F51C97ADB00523BD214C653C
SHA-256:	78EB4A3213EBE7BB95F87D206AE29064D514628E6A430334D0E13756AA131DE5
SHA-512:	A0C70871BC52467524A0107F09B93C1BE11FFBD9CF68E1F3C567F97B0F810AA5B0CEE584AE1BA720F4A0B30F42E4290A06E99B9EA640437B0DABF158F2DB062
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_1920x1080.jpg&rf=LaDigue_1920x1080.jpg
Preview:	......JFIF.....C..... "" .,,,.3333333333...C..... ....## ##,,),.3333333333.....8...."..... .....S..... ....!1A.."Q2aq..B...#R...b.3r....$C.....4Scs..%DT…u.5t.....B.....!..1AQ."aq.2.....BR..#br.$34..C....Ss...c.....?.#...9.%qx..fL.Z..+p.....+...X .2m..,..X.<..W...}Dk.\J....f9.~.....b.../.7C&.V.Y.9`.|.rV0'>.9.....3._>.6.@...ML-...+].Q.....]....'>.`e..W>.9.....|.d...>.9..VJ.Es./.%e....,..y.7.....l.....g.4.3g)..d.99Bk....+r. :e$.ca.SH.|.....m...}.YRO9...j.vd..9V..5..@e...{.<hA...:.....9K#.....q.H...`....q>NiF=.[..2C.8X...*.....L(.{.....s.3.W.!....{^..'..~....9.!..^A.y...1.A..[.....l!a....i ..)L.D.D.8#.{../.0.\.M. .r..qg3...t.N..^....L.I3'.....eQ.`3{.....Yh...sK...k..I...m.o.t^%e...O..e&a.....9..v.x....&.E!.e..p.....n.UQ.x$S\.....1}DqH

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[2].jpg	
Category:	downloaded
Size (bytes):	5038
Entropy (8bit):	7.913300499070733
Encrypted:	false
SSDEEP:	96:pPEvzuSDKiT+ERod8yBN0X/HmlRJJ+Fn8h3fzh+LZvwk:pPOCSmHhW/H4JJ+F8xzh+L9wk
MD5:	B4253CC44B582EBE891CBCDF0EF5CA8B
SHA1:	2D179CB4C761077F9EFB53625FE0B34D01AE3107
SHA-256:	9358906D6A9154E881A96AA4E9EDED3CCFDF3DC87B1B922B8FC4C09B970130F5
SHA-512:	6D3EA094D383E370E85CBDD445B76D8B2986B3F175145F8DB93112A63E48DF8FA1877BBFD25C2CA73CE66B2C1DECF7FAB01D9556855CF9DD1F9462D4432F60B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flcl7.img&ehk=n4zxNzUaGmaWvZYudQOxjiEm8O7nfdAvG5P6LGtz8zo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..(...).C$..$gbp..z=.P..`Tz...i.&..+nO._...f7'.....:.....[..zf..a..E.U.(...(...(...(...(.6v.....!..V.k.@.....N...>...Rxc.7:.i.....#.cz..k.4..[i6...bL1c...../.8./.Iob.D+....#,.s..O.I..U7.....z|.i2m.Y...[..j.....Xjodp'HXG..sw>.kJ...Fv2..(..z...D.9L.....b..-./..'....U....t..:}...DV-.u....>u..y...b...Xn.)' ..:.....<>t.e..0...U....=.oN..f...8.(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	2542
Entropy (8bit):	7.7794956985553245
Encrypted:	false
SSDEEP:	48:5yYcuERATBsC87tpyXKeyzbOZkEPVEGYI0Z8RV8WdxGAia:5PECCC87jyXK7ejRWSRV/dxGva
MD5:	357F88390923FD2D7C54F8EF73A57475
SHA1:	EE6F5D3CBE310AC210CF47D8F1B748B2B0B5205E
SHA-256:	80076FB2A8BD57B72985F5F3557F2B4742DE360994CD05CCA6604653E63404E0
SHA-512:	2AE5C52C81E088CEA10B4240BDF45220AEAC3C4BFDEEC6C098F946BA569AE626E753F7CC116FF133C920C14DBC94083B484A3FA045EC226A32F62D69F85D05C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fl5aC.img&ehk=hx9sEjlDgrlxhlQ0dXS9BWLt7M4%2fn9L%2foLPShsm8wa4%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..(...7..(.....d..0..ci.0.H.8.4ow;F..b[ws.....q...r..@...3L_7..?n.....?LV..d?...J+".....)(.....E8.....W.....F,..JZ..Z)(.....J...fv.....@$...0.cn..q.N{g..:....RCp..2aG.ll.T..S.....w .9..V...h.E..aE.....(...(..4.J..K../J(N.WB1{..E..l-....(4Q@...[M.0.....18....[..Z.....W.J._.#...;s.q...v.....W.l+kr.-%.#.(...(...(...j`<..:.[.a:QH.WJ1{.....c`.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	3792
Entropy (8bit):	7.879458150606813
Encrypted:	false
SSDEEP:	96:pPEUZavUpaPPjl0qwzhf5Q6u2i7HGLHFgak2bB+u+iiKaCPg8o:pPH0vUWlqhf5Q6uZiDFgak3neaFF
MD5:	E5D2688116BA8D4ABBC53F2493A181BE
SHA1:	2330F5A38AB1DE6979790C84B33DC173F853D6FD
SHA-256:	AA1EF9A296A78952F642406AA0F59930CDD23BC5D1714B7E306787CD4064229E
SHA-512:	0FEBAA0286AFF016B5F0B2B9984D95E2319CA29E41AF624A50D5BF1EDA33CD61017226312DE65B1E5A169A95DB7A6F9212EFFC06A498B0BA857C744CCCBDE3BA
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flaPv.img&ehk=nfyoU%2b8cc2O%2frjxfHaxiAbz0t%2fXYbGhU6jS%2bwZAdcS0%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....``.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..x.[.G....uz.....M8.....4..l..2..?..9....$q..r./...LE....'o...w.[H.J..Z..G..Nl.....gC..pk.n..hF.+..<..V...d).....,..Bpj.DT...Rl-..@...i..L.....e.*&(..`...P...l..J...@.Mqc}z.....>..)U,y.^.Aq...X...QG.8W....Q..]^..j.|.n~X...[.....\.n.i0..#..9..<Wk.....bx.._.....idb3.A..k7+.....,.M./..@...2.?.Y}M....$.....)=....w]....>Y..t+.I....Z.9$.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[5].jpg	
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4602
Entropy (8bit):	7.919085409507157
Encrypted:	false
SSDEEP:	96:pPEQIac5U07wxonYM7ZCOPHZ3V4DItC+Es/YzbvLSLIBpxrDn5M:pPjeyynnlCoZ32In4TL6CHD+
MD5:	8816AF91855EFB0BB97FAF7429A17E5A
SHA1:	7FFA5A24554D8CA448E6D1F98A7AC31F36CB2FC7
SHA-256:	1C54DB3F6FA0501AB0C6ACC1BFFC8629009F76BE5AA6DE4239FEB24E3C6AEBFC
SHA-512:	F615D37B9E117B9E1A8DC287DC4FD5888BE85F8CB9E9C66E49B547A0D3969611771660322511 7D05D7E30734131D15A5C651EFD0B6E9DA546825352B25CCF082
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fjIfk.img&ehk=fogkfx9NpBv%2brwC9WfPL2X5KtkEuDG5AjpDW%2f%2bCifdo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..XqBS.N)..i.,'..H..uH..(..(..5H..$..$...u$...j^/..]4.[...h.).z.V...+.jt1.7E'.).V/.....O...(..c.....8...!ei.|.Y.py...4...=...y_Q.....R{G2Z\4,9'".....7.iz.>..p..zP..lz.)....<J.z..P..OZn).H.....h.4P..>(.. S$..J.&.P...(.....e...Py.....mjH...}.#.u..g..@.'.j...v.r.zd..kR..[...$.p.....P.....".b|...9.....8_A.....9.i[J.Y.(#..[.:Ai.<".....k...;d.j:w.\.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\MEEXW4H4\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6795
Entropy (8bit):	7.939267233088054
Encrypted:	false
SSDEEP:	192:pPFWzMAm+TL7LZ895qWynOjJN52aPjP2D9a1R0:5FWmM7y7TZFNoaLc9Ai
MD5:	140F382635756FE19E1CD67D8CDAB923
SHA1:	1B0F1B61C068E01CE6FFDC5FFCADDD5E039D0DA5
SHA-256:	216E799943B615F3EBF0FC09391810AF53FDE0EDCBEC4300F2B01B98AF346FAE
SHA-512:	A7403C2FB1E2C858C3B3A1F6860441A8B820033E5D6E0049DF6922A1BFB0F74180A2538CFD82F292219629FB1FCA6AB8D3AAAA97129C4C86BC8D15FACDD405F3
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk3tJ.img&ehk=VNetxfVLBzRQk0Hk9PeD6wuxhnc6QG%2bQVORzTT762Ms%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=========..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...3Fj.E.[.$\..M..+.ij.!...{..,.....j\..|.\....>..7.....}kVo.(bD..U...Pj....XO.....$.[..|....<...p._0..n*...k..O...D6.L.`....?..U-..D...f.....h.'z^(...&j...[h:S..."..... ....O.k.o...7..@..`.n.~R.....Px...m ;.3X...E.....D..Cm.$..8>....F(...VrB.1..4S.....u.&.w.Oe3...1.C..2.....1..5.j.....!&._..n.h...'.r.=I..y...Y..2.\....a$...$.;.$..v..,.....YR..%.....;.N

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\1CAOP5TZ.htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, UTF-8 Unicode text, with very long lines, with CRLF, LF line terminators
Category:	downloaded
Size (bytes):	60850
Entropy (8bit):	5.75998311469477
Encrypted:	false
SSDEEP:	1536:GKrSCXrLQPo3H/8cpUQbcqETOuKsIecFXdAjvd894fJLYvIMNeb097Q53Opw:GGLQw3f/mQYbd89RYew
MD5:	100FFBA8DF106CB6BD7434D4B0AFBC41
SHA1:	720150A7BC749C1BCA375298D27EF4C8CBFF82E8
SHA-256:	48B60D30ADE5263B2ECAB01C85923C441F6501130624D74FDB4AC68FA92DDDB1
SHA-512:	B1ABF810CF62599575EE395896A11F500FF0B516B9B15097892DA70A47E97EB63FF9D5E551C5C98E5D354F05D4337B1F07AA90F1845FF9CF75CF5DB5EB3824B7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/?form=REDIRERR
Preview:	<!doctype html><html lang="en" dir="ltr"><head><meta name="theme-color" content="#4F4F4F" /><meta name="description" content="Bing helps you turn information in to action, making it faster and easier to go from searching to doing." /><meta http-equiv="X-UA-Compatible" content="IE=edge" /><meta name="viewport" content="width=device-width, initial-scale=1.0" /><meta property="fb:app_id" content="570810223073062" /><meta property="og:type" content="website" /><meta property="og:title" content="Info" /><meta property="og:image" content="https://www.bing.com/th?id=OHR.Olympics125_ROW9889344454_tmb.jpg&rf=" /><meta property="og:image:width" content="1366" /><meta property="og:image:height" content="768" /><meta property="og:url" content="https://www.bing.com/?form=HPFBBK&ssd=20210406_0700&mkt=de-CH" /><meta property="og:site_name" content="Bing" /><meta property="og:description" content="The first modern Olympic Games were held 125 years" /><title>Bing</title><link rel="shortcut i

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	SVG Scalable Vector Graphics image

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\5rqGloMo94v3vwNVR5OsxDNd8d0[1].svg	
Category:	downloaded
Size (bytes):	461
Entropy (8bit):	4.834490109266682
Encrypted:	false
SSDEEP:	6:tI9mc4sl3WGPXN4x7ZguUz/KVqNFvneuFNH2N9wF+tC77LkeWVLKetCsYuwdOvX0:t41WeXNC1f3q/7H2DlZWYeIsrGYyKYx7
MD5:	4E67D347D439EEB1438AA8C0BF671B6B
SHA1:	E6BA86968328F78BF7BF03554793ACC4335DF1DD
SHA-256:	74DEB89D481050FD76A788660674BEA6C2A06B9272D19BC15F4732571502D94A
SHA-512:	BE40E5C7BB0E9F4C1687FFDDBD1FC16F1D2B19B40AB4865BE81DD5CF5F2D8F469E090219A5814B8DAED3E2CD711D4532E648664BFA601D1FF7BBAA83392D30E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/5rqGloMo94v3vwNVR5OsxDNd8d0.svg
Preview:	<svg xmlns="http://www.w3.org/2000/svg" viewBox="0 0 32 32"><title>UserSignedOutIcon</title><circle cx="16" cy="16" r="16" fill="#eee"/><path d="M12.73 13.1a3.271 3.271 0 1 1 3.27 3.2 3.237 3.237 0 0 1-3.27-3.2zm-2.73 9.069h1.088a4.91 4.91 0 0 1 9.818 0h1.094a5.884 5.884 0 0 0-3.738-5.434 4.238 4.238 0 0 0 2.1-3.635 4.366 4.366 0 0 0-8.73 0 4.238 4.238 0 0 0 2.1 3.635 5.878 5.878 0 0 0-3.732 5.434z" fill="#666"/><path fill="none" d="M0 0h32v32h-32z"/></svg>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\BJp5dDFvoQm12CHBfp4PC6aiyg4.gz[1].css	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	73202
Entropy (8bit):	5.307816444057117
Encrypted:	false
SSDEEP:	1536:kcGJTL/mKzAAFl7JlsG0GRe1cxnoWC1kuyOYkTs/Kun:LGJ4AFl7JlsG0GRCcxnoWC1kuyOYkT0
MD5:	C912DA2683E71660357A600EE34A7873
SHA1:	5DFD028307D4CD8A66492E807B848FEC177AEC3A
SHA-256:	525D57B5D38D8212993C66A33F4CD15EDBD0F260A5AFCF539D092047A908D6EE
SHA-512:	31E2A56C27CC037AD903292DFA518E86642C2A610E9923DD4F7A2FD1347167E042E957A85E98561CC9178318D121DEA3EF165F88EEC79915D0687939DC25BBC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/BJp5dDFvoQm12CHBfp4PC6aiyg4.gz.css
Preview:	.scopes{color:rgba(255,255,255,.8);display:inline-block;left:0;white-space:nowrap;list-style:none;line-height:39px}.scopes.sc_hide{display:none}.scopes .scope{font-size:.8125rem;cursor:pointer;vertical-align:middle;margin-right:36px;background-repeat:no-repeat;position:relative;display:inline-block}.scopes .scope:hover,.scopes .scope.focusin{color:#fff}.scopes .scope:hover .overflow_menu,.scopes .scope.focusin .overflow_menu{transform:none}.scopes .scope:focus-within .overflow_menu{color:#fff;transform:none}.scopes .scope a{color:inherit;cursor:pointer;text-decoration:none}.scopes .scope.dots{margin-bottom:8px;font-weight:bold}.scopes .scope.dots:before{display:inline-block;content:'. . .'}.scopes .scope.dots.hover_focus:focus{outline:none}.scopes .scope .overflow_menu{color:#666;cursor:pointer;transform:scale(0);position:absolute;background-color:#fff;border-radius:6px;padding:4px 0;box-shadow:0 4px 12px 1px rgba(0,0,0,.14);min-width:155px}.scopes .scope .overflow_menu .overflow_item{

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\GiGr-rA9TBhE2c3LJn7PvDweiOo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	374771
Entropy (8bit):	5.158592433297743
Encrypted:	false
SSDEEP:	6144:1irrzbB3LH7gaV6Z8LAfP0Rp6Izc04YFdNwRm2EjXi4SG7oIBYQmzeH:aHNfi4KwYQmzeH
MD5:	F279A46B56038C41BB3FC11D67D0FE46
SHA1:	B48121E695FD6483CAA7F48DE73FE9F121777109
SHA-256:	A9EA274B393E34591387AC0B4DE594BEE296386543DE34F4897281324DB0DCBB
SHA-512:	4C1754CF5E368D8CE86B135B789A4FF4BAAD1419F30A1EB3B65EAB62217C054D0066EA5FC22B5AA7643EA959854EBC2029B39CB7D1AEAAFB78B95A2A46430F84
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/GiGr-rA9TBhE2c3LJn7PvDweiOo.gz.js
Preview:	(function(n){function t(r){if(i[r])return i[r].exports;var u=i[r]={i:r,l:!1,exports:{}};return n[r].call(u.exports,u,u.exports,t),u.l=!0,u.exports}var i={};return t.m=n,t.c=i,t.d=function(n,i,r){t.o(n,i)||Object.defineProperty(n,i,{enumerable:!0,get:r})},t.r=function(n){typeof Symbol!="undefined"&&Symbol.toStringTag&&Object.defineProperty(n,Symbol.toStringTag,{value:"Module"});Object.defineProperty(n,"__esModule",{value:!0})},t.t=function(n,i){var r,u;if((i&1&&(n=t(n)),i&8)||i&4&&typeof n=="object"&&n&&n.__esModule)return n;if(r=Object.create(null),t.r(r),Object.defineProperty(r,"default",{enumerable:!0,value:n}),i&2&&typeof n!="string")for(u in n)t.d(r,u,function(t){return n[t]}.bind(null,u));return r},t.n=function(n){var i=n&&n.__esModule?function(){return n["default"]}:function(){return n};return t.d(i,"a",i),i},t.o=function(n,t){return Object.prototype.hasOwnProperty.call(n,t)},t.p="",t(t.s=0)})([function(n,t,i){window.SpeechSDK=i(1)},function(n,t,i){"use strict";function r(n){for(

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1516
Entropy (8bit):	5.30762660027466

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz[1].js	
Encrypted:	false
SSDEEP:	24:+FE64YTsQF61KWllWeM2lSoiLKiUfpIYdk+fzvOMuHMH34tDO8XgGQE3BUf4JPwk:+FdF6UYXEBi9kIHIB1UY
MD5:	EF3DA257078C6DD8C4825032B4375869
SHA1:	35FE0961C2CAF7666A38F2D1DE2B4B5EC75310A1
SHA-256:	D94AC1E4ADA7A269E194A8F8F275C18A5331FE39C2857DCED3830872FFAE7B15
SHA-512:	DBA7D04CDF199E68F04C2FECFDADE32C2E9EC20B4596097285188D96C0E87F40E3875F65F6B1FF5B567DCB7A27C3E9E8288A97EC881E00608E8C6798B24EF3F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/P3LN8DHh0udC9Pbh8UHnw5FJ8R8.gz.js
Preview:	var Identity=Identity||{},ham_id_js_downloaded=!1;(function(n,t,i,r,u,f,e){e.wlProfile=function(){var r=sj_cook.get,u="WLS",t=r(u,"N"),i=r(u,"C");return i&&e.wlImgSm&&e.wlImgLg?{displayName:t?t.replace(/\+/g," "):"",name:n(t.replace(/\+/g," ")),img:e.wlImgSm.replace(/\{0\}/g,f(i)),imgL:e.wlImgLg.replace(/\{0\}/g,f(i)),idp:"WL"}:null};e.headerLoginMode=0;e.popupAuthenticate=function(n,i,r){var o,u,h,c,v=sb_gt(),l=Math.floor(v/1e3).toString(),s="ct",a=new RegExp("([?&])"+s+"=.*?(&|$)","i");return n.toString()==="WindowsLiveId"&&(o=e.popupLoginUrls,u=o[n],u=u.match(a)?u.replace(a,"$1"+s+"="+l+"$2"):u+"?"+s+"="+l,e.popupLoginUrls.WindowsLiveId=u),(o=e.popupLoginUrls)&&(u=o[n]+(i?"&perms="+f(i):"")+(r?"&src="+f(r):""))&&(h=e.pop(u))&&(c=setInterval(function(){h.closed&&(t.fire("id:popup:close"),clearInterval(c))},100))};e.pop=function(n){return r.open(n,"idl","location=no,menubar=no,resizable=no,scrollbars=yes,status=no,titlebar=no,toolbar=no,width=1000,height=620")};var o=u("id_h"),s=u("id

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Passport[1].htm	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	HTML document, ASCII text
Category:	downloaded
Size (bytes):	329
Entropy (8bit):	5.086971439676268
Encrypted:	false
SSDEEP:	6:qzxUe3X965+zAqEFtTNfYEAn4TXQ3SOFCL0H4WZhCroOI:kxFkXq6tTRYEVTAx4IHH7CroOI
MD5:	7B7D5DA1B057EB0D5A58C2585E80BACA
SHA1:	29714CD8C570E321C1C1C991E77ACE3945312AC6
SHA-256:	023CD9B7315636BE1BE24DC78144554B0E76777BD476ED581378172DE9B12A05
SHA-512:	1A4E36E3124968166579C04D05A1325242E1DFE20DF4C804081487A019B88395A679A439525488F78B73334C5B0BD38D61E24F8E23F2F8274C6BAC323291CEE8
Malicious:	false
IE Cache URL:	http://https://www.bing.com/secure/Passport.aspx?popup=1&ssl=1
Preview:	<html><head><title>Bing</title></head><body>Loading...<script type="application/x-javascript">//<![CDATA[.var _w = window; var o = _w.opener; var mainWindow; (mainWindow = o) || (mainWindow = _w.parent); if (mainWindow) {mainWindow.sj_evt && mainWindow.sj_evt.fire("wl:cancel"); };if (o) _w.close();;.//]]></script></body></html>

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4140
Entropy (8bit):	5.268233767834181
Encrypted:	false
SSDEEP:	96:cithlPK4kMRX+1XewlYONYyuGNc22nDmSOsDg:ciJALYONEGNc22nbOsDg
MD5:	7651609B4BE35F5DE8024F570EF6CF87
SHA1:	4B72E4BB1D8F170D6B17FA1D769584A7D0F02F70
SHA-256:	4CA5C607D14D17F8A9EEA9FB0A624BC00C49BFDFBB6A78E1292EAE1461B7D9F0
SHA-512:	7BE114BD02AA079F01FBFC343811F74896BB247ABB79C67998B7DB0F20F8ED1260DEA83523F61CDD0E2231F2428437F9FBF88F39DAD821A3F09A5116C5DA7A2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/RrvsBuqGHDpqG7NAz4Q0BMOqQBg.gz.js
Preview:	var Feedback;(function(n){var t;(function(){function r(i,r,u,f,e,o){i=typeof i===t?!1:i;i&&scrollTo(0,0);u=typeof u===t?!0:u;n.PackageLoad.Load(r,u,f,e,o)}function e(n,t){for(var r=0,i=null;n&&n.getAttribute&&(!(t>=1)||r<t);){if(i=n.getAttribute("data-fbhlsel"),i!=null)break;r++;n=n.parentNode}return i}var u="feedbackformrequested",c="feedbackInitialized",i,f="",o="feedback-binded",s="clicked",t="undefined",h;n.Bootstrap.InitializeFeedback=function(l,a,v,y,p,w,b,k){function tt(t){var r=null,i;return t&&(i=new h,n.fel("ajax.feedback.collectsettings","gsf",i),r=i.findSettings(t)),r}var d=_ge(a),g,nt;d&&d.classList&&d.classList.contains(o)||(p=typeof p===t?!1:p,g=e(d,3),f!=="sb_feedback"&&(f=a,typeof sj_evt!==t&&(i&&sj_evt.unbind(u,i),i=function(n){var u=null,t=null,f=null,o,i,s;n&&n.length>1&&(i=n[1],i.tagName!==undefined&&i.nodeType!==undefined?(u=i,t=tt(u)):t=i,o=t&&t.elementToHighlight||u,f=e(o));s=t&&t.linkId||a;r(y,l,v,s,f,t)},sj_evt.bind(u,i,1)),typeof SearchAppWrapper!==t&&SearchA

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	576
Entropy (8bit):	5.192163014367754
Encrypted:	false
SSDEEP:	12:9mPi891gAseP24yXNbdPd1dPkelrR5MdKIKG/OgrfYc3tOfIvHbt:9mPlP5smDy1dV1dHrLMdKIKG/OgLYgtV
MD5:	F5712E664873FDE8EE9044F693CD2DB7
SHA1:	2A30817F3B99E3BE735F4F85BB66DD5EDF6A89F4
SHA-256:	1562669AD323019CDA49A6CF3BDDECE1672282E7275F9D963031B30EA845FFB2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\Xp-HPHGHOZznHBwdn7OWdva404Y.gz[1].js	
SHA-512:	CA0EB961E52D37CAA75F0F22012C045876A8B1A69DB583FE3232EA6A7787A85BEABC282F104C9FD236DA9A500BA15FDF7BD83C1639BFD73EF8EB6A910B75290D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/Xp-HPHGHOZznHBwdn7OWdva404Y.gz.js
Preview:	var SsoFrame;(function(n){function t(n){if(n&&n.url&&n.sandbox){var t=sj_ce("iframe"),i=t.style;i.visibility="hidden";i.position="absolute";i.height="0";i.width="0";i.border="none";t.src=decodeURIComponent(n.url);t.id="aadssofr";t.setAttribute("sandbox",n.sandbox);_d.body.appendChild(t);n.currentEpoch&&sj_cook.set("SRCHUSR","T",n.currentEpoch,!0,"/");Log&&Log.Log&&Log.Log("ClientInst","NoSignInAttempt","OrgId",!1)}}function i(n){try{n&&n.length===2&&t(n[1])}catch(i){}}n.createFrame=t;n.ssoFrameEntry=i;sj_evt.bind("ssoFrameExists",i,!0,null,!1)})(SsoFrame||(SsoFrame={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\eF3rIdIG4fsLyPy7mzgRnjCDKIA[1].png	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 1642 x 116, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	12172
Entropy (8bit):	7.918443542633748
Encrypted:	false
SSDEEP:	192:55tSglBjXtk3RBPvjc6/sB7WYFH+CEWAY7ajZiS8aQoFiJ8VJUsLYpP7:YHHjNsB7WYtFEV1iS8XoFRJbLmP7
MD5:	4CF2646B3478E81FB9444ED499C19310
SHA1:	785DEB21D206E1FB0BC8FCBB9B38119E30832880
SHA-256:	3E3D1F762BE8E3AF89D77E1F291E6228D55FBA619AD6C0763224B4A640D0D9BD
SHA-512:	6CC812012B23313ED2A83706D81B9737C3C6D8EA656FFE8D612006C4C6C03ACCA8428D4C2F89615581F1ACD866925F6DA94F2C66275101558DC8D202E976479
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eF3rIdIG4fsLyPy7mzgRnjCDKIA.png
Preview:	.PNG.....IHDR...j...t.....PLTE...ttt"""".....""""///...,,,000....}.....*x.%..$..#..$.""",,,....Q".L"~..~.....*:*.....#.....".....---.....O.#.+++.....---.....$.....y..`..G.....).....wwwttt...[[[.....413.....vwzlllqqq.....rxxvxy...vwy.....vwy.....!W.....Y..4f.....uwzwxz.....xxxwxzwwzvvzvwy...vxz.3..0.....l..m..4.....".3.....2..3..l..4.....3..3.....d!.a...?..>..=wxyvwyvwyvv{wxxwxzvxz]ffwwyvwzwwwwxzvxzvxywwzwxzvwzwwzwxzwwzvxywwy..>.....!....tRNS..C.....`....C...1.....P.....P.....$`.....@.....j.0.G..p. p.@.`+.``..>^.`..... k@.@.P..p.....0... .....P....``....i...@.. ..0@.....^f....P.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\errorPageStrings[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	4720
Entropy (8bit):	5.164796203267696
Encrypted:	false
SSDEEP:	96:z9UUiqRxqH211CUIRgRLnRynjZbRXkRPRk6C87Apsat/5/+mhPcF+5g+mOQb7A9o:JsUOG1yNlX6ZzWpHOWLia16Cb7bk
MD5:	D65EC06F21C379C87040B83CC1ABAC6B
SHA1:	208D0A0BB775661758394BE7E4AFB18357E46C8B
SHA-256:	A1270E90CEA31B46432EC44731BF4400D22B38EB2855326BF934FE8F1B169A4F
SHA-512:	8A166D26B49A5D95AEA49BC649E5EA58786A2191F4D2ADAC6F5FBB7523940CE4482D6A2502AA870A931224F215CB2010A8C9B99A2C1820150E4D365CAB28299
Malicious:	false
Preview:	.//Split out for localization...var L_GOBACK_TEXT = "Go back to the previous page.";..var L_REFRESH_TEXT = "Refresh the page.";..var L_MOREINFO_TEXT = "More information";..var L_OFFLINE_USERS_TEXT = "For offline users";..var L_RELOAD_TEXT = "Retype the address.";..var L_HIDE_HOTKEYS_TEXT = "Hide tab shortcuts";..var L_SHOW_HOTKEYS_TEXT = "Show more tab shortcuts";..var L_CONNECTION_OFF_TEXT = "You are not connected to the Internet. Check your Internet connection.";..var L_CONNECTION_ON_TEXT = "It appears you are connected to the Internet, but you might want to try to reconnect to the Internet.";....//used by invalidcert.js and hstscerterror.js..var L_CertUnknownCA_TEXT = "Your PC doesn\u2019t trust this website\u2019s security certificate.";..var L_CertExpired_TEXT = "The website \u2019s security certificate is not yet valid or has expired.";..var L_CertCNMismatch_TEXT = "The hostname in the website\u2019s security certificate differs from the website you are trying to visit.";..var L

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	443
Entropy (8bit):	4.86644754379557
Encrypted:	false
SSDEEP:	12:kdXCJAUQECJA5MeMJA561cnGfbs4Hbrk86fYXChdJAjU:8CJWECJKMeMJK61cuo47rk8WYMdJyU
MD5:	56583BD882D9571EC02FBDF69D854205
SHA1:	8DFF13B78F4CBCC482DC5C7FC1495390200C0B94
SHA-256:	DF0089A92B304A88F35AA0117CF8647695659AAF68B38B1B7A72A7C53465E9C7
SHA-512:	418B3003B568F2FDB862035EE624CE93087861AEBB6680CDC0E0F1212297B64D30596EEF931B8C6E818292C4AB14C8C17FF0BAF9E58ED93392AD7A80621EBBE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hqx6FcD0hjfzrON5oLgx2RMMD1s.gz.js

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\hqx6FcD0hjfzrON5oLgx2RMMD1s.gz[1].js	
Preview:	var OutlinePolyfil=function(){function n(){var n=this;this.attachHandlers=function(){n.attachHandlersForOutline()};this.attachHandlersForOutline=function(){addEventListener("keydown",n.onTabKey);addEventListener("mousedown",n.onMouseDown)};this.onTabKey=function(n){n.keyCode==9&&document.body.classList.add("tabbing")};this.onMouseDown=function(){document.body.classList.remove("tabbing")};this.attachHandlers()}return n}();new OutlinePolyfil

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	downloaded
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
IE Cache URL:	res://ieframe.dll/httpErrorPagesScripts.js
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\k5oM71-Oyo7w7ptkcB_2S5dlr7I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with CRLF line terminators
Category:	downloaded
Size (bytes):	21824
Entropy (8bit):	5.243380331742482
Encrypted:	false
SSDEEP:	384:HXpeDC+2uguwBYFsOZrSzz3wp0OxAmzjEHU:HXpeDz2gFsOZrOXWz4HU
MD5:	071CABC528DA3CDD5BD5C7F0EC48ED96
SHA1:	8B665A2DA630D6711E01E838877510F48C40E9CE
SHA-256:	9871F6289648EEA5CB484C2307C4E7BCDF3857AEB27EB07E0ACFD4C1B77EDBB5
SHA-512:	771DA4D3B22B53C5B1B1D2DF1B923B78124A7F92576700F7E988A1E40C2806CB2366D52C556F1FD49862B1A584D871ED7207B54174172740B4ED125AAD4C531F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/k5oM71-Oyo7w7ptkcB_2S5dlr7I.gz.js
Preview:	(function () {.. if (typeof window !== 'undefined') {.. (function (arr) { arr.forEach(function (item) { if (item.hasOwnProperty('remove')) { return; } Object.defineProperty(item, 'remove', { configurable: true, enumerable: true, writable: true, value: function remove() { if (this.parentNode === null) { return; } this.parentNode.removeChild(this); } }); }); })([Element.prototype, CharacterData.prototype, DocumentType.prototype]);.... !function(e,n){"object"==typeof exports&&"undefined"!=typeof module?n():"function"==typeof define&&define.amd?define(n):n()}(0,function(){"use strict";function e(e){var n=this.constructor;return this.then(function(t){return n.resolve(e()).then(function(){return t})},function(t){return n.resolve(e()).then(function(){return n.reject(t)})})}function n(e){return!(!e||"undefined"==typeof e.length)}function t(){}function o(e){if(!(this instanceof o))throw new TypeError("Promises must be constructed via new");if("function"!=typeof e)throw new Type

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\pXscrbCrewUD-UetJTvW5F7YMxo.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	511
Entropy (8bit):	4.980041296618112
Encrypted:	false
SSDEEP:	12:yWF4eguIWKvU9bEMsR5OErixCvJO1Vi5rgsM:LF4mKctEMYOK4CvJUVYM
MD5:	D6741608BA48E400A406ACA7F3464765
SHA1:	8961CA85AD82BB701436FFC64642833CFBAFF303
SHA-256:	B1DB1D8C0E5316D2C8A14E778B7220AC75ADAE5333A6D58BA7FD07F4E6EAA83C
SHA-512:	E85360DBBB0881792B86DCAF56789434152ED69E00A99202B880F19D551B8C78EEFF38A5836024F5D61DBC36818A39A921957F13FBF592BAAFD06ACB1AED244E
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/pXscrbCrewUD-UetJTvW5F7YMxo.gz.js
Preview:	var BingAtWork;(function(n){var t;(function(n){function t(t,i){var u,r;t.isAuthenticated&&(n.raiseAuthEventAndLog(t),u=_ge("sb_form_q"),u&&(r=u.getAttribute("value"),r&&(n.fetchLowerHeader(r),n.fetchScopeBar(r),i.notifEnabled&&i.notifFetchAsync&&n.fetchNotificationConditional())))}function i(n,i){n&&n.length==2&&t(n[1],i)}n.bindToConditionalSignIn=function(n){sj_evt.bind("ssofirstquery",function(t){return i(t,n)},!0,null,!1)}})(t=n.ConditionalSignIn||(n.ConditionalSignIn={}))})(BingAtWork||(BingAtWork={}))

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\swyt_VnIjJDWZW5KEq7a8l_1AEw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2298
Entropy (8bit):	5.34865319631632
Encrypted:	false
SSDEEP:	48:KWEkTScZVcMBOwXhzwBi88RnX8ec0T39B8onA008xG9FLCx3w0S5xJ:KWEkTDZVXpR0BiXjTtB8mA0zxWsx3PG/
MD5:	A8D7D1B3681590980B2D7480906078DB
SHA1:	C9A7A400DB1EBAD4DCA028546EE5F5B2EF4136BD
SHA-256:	1390485DC88B6230389D9C95232A3710BF38D47271708A279B12D7E68E43F649
SHA-512:	710D31EFD76614EC4C94888E2FCC49ABAB50EF406FC0F1C5C10D8AA21D4E9F349DE78068B2BAFE495C074AB4E6EC0A5D44EB5506B2D79C78707A23C1D8206664
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/swyt_VnIjJDWZW5KEq7a8l_1AEw.gz.js
Preview:	var Bnp=Bnp||{};Bnp.Global=Bnp.Global||{};Bnp.Version="1";Bnp.Partner=Bnp.Partner||function(){function u(n){sj_evt.fire("onBnpRender",n)}function i(n){var r=r||{};if(typeof r.stringify=="function")return r.stringify(n);var o=typeof n,u=n&&n.constructor==Array,f=[],e,t;if(o!="object"||n==null)return o=="string"?""+n+"":String(n);for(e in n)t=n[e],t&&t.constructor!=Function&&(u?f.push(i(t)):f.push(""+e+":"+i(t)));return(u?"[":"{")+String(f)+(u?"]":"}")}function o(n){for(var r=[],u=n.getElementsByTagName("script"),t,i;u.length;)t=u[0],i=sj_ce("script"),t.src?i.src=t.src:t.text&&(i.text=t.text),i.type=t.type,t.parentNode.removeChild(t),r.push(i);return r}function s(n){for(var t=0;t<n.length;t++)f(n[t])}function f(n){t=t||_d.getElementsByTagName("head")[0];t.appendChild(n)}function h(n){for(var t,i=0;i<n.length;i++)t=sj_ce("style"),t.type="text/css",t.textContent!==undefined?t.textContent=n[i]:t.styleSheet.cssText=n[i],f(t)}function c(){sj_evt.fire("onPopTR")}var n="dhplink",t,e=2500,r=

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4355
Entropy (8bit):	7.900585011984252
Encrypted:	false
SSDEEP:	96:pPE2WJmwonMcP1FpJlLr+clrDFU1Zgk6qe:pPqJfvcPzlpIrDMOk6qe
MD5:	A8AF8B0E212D16641FFF14C692653A31
SHA1:	7F43B7DB65F94F5579B8F338EAEF385F3582573C
SHA-256:	DCA522E3D710326E3009DBEAFD627F940907F615F9922201F636D6352DF50A77
SHA-512:	943633BF7A4E4ABBD086DA138FA68D23A0889CFE815505D641F907241506FB3C9324D6C289F3FE42D86480426F3B8F467AEF1B86626018AD6DC22D47FD1ACF3A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flnql.img&ehk=e56b2FA%2fdQ8S1%2bJCLPLA5GewBcl71RQ%2fTmEAxvevKks%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....H.4.(..J.(..P.....\P.R...p.I.(....ej^%..v.,\L.6.S.....hu}N..X.D=...5..Z.F.....B+%u....E ...U.MN.....<..~.....D.E4...i. ..H....LdDTdT.TI)...)....O...<.d...(.... ..1KH..ex..[M0El..o%.y.....Z...n.0TE,.z(.$.+{.G....$.G..z6{.9.'b....4.,U.UY.....k&.2...sZP.:g..Z.6.$..J..+'Q....E2....-.....a.^5....*..7.z.cW.bi..n...H..?..Z.S.+1..i.E2F.Q..M1..!".q..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4858
Entropy (8bit):	7.912860451432217
Encrypted:	false
SSDEEP:	96:pPE/rJtrOaBegYjEZcV2CWr45p5VrbFU4/PbFI+tMpg:pPYKaBeXE6d59bLui
MD5:	C27EAAD7FDCAD067348EB8426A6643DD
SHA1:	D5362D86359F58F1F08EBC9E9F7627F61CB70909
SHA-256:	20EA77BAF0828E450BB7EB0895759B7C760D1F4C00B1EF5366F91B2F23B30429
SHA-512:	AF46A7A9FAEF467FBBA40194C4B8E6A57EDF476ACC10CBEE4CADF87E8CFFA5DBCCB6EC6601944724148F59E8EBCB317442F88BE272657EC4A9EDC841B984FBD2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGpp.img&ehk=EoXsvHvTz25OeDlk8%2f1AsQ0JRbPiNyy0iD13c2N9OGI%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..%8&jP....p..u..p"..z....e.....`.1...:.....J.O3.....k.....6I.J0..1..&K..(P...GS[..b.(."....`zT.....I...3..}g<ig.M.r....~5.....[.....sz.f^.....(^Cg..{...1.....n1.`..A.*.I....m+;Gx.....3..q[..!.p.....G..>VrU.+..).*..iZ.9lU)L)V.SJS$.R.V...2S..J.E...]...sEJR..:5L... ....)..@..s]|i..W..d7.<k.v.=z.....p.=l..,L.]....4...L..c.Q....j..}.%.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[3].jpg

File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6319
Entropy (8bit):	7.921601448672384
Encrypted:	false
SSDEEP:	96:pPE3Um+CGqdS0RiboPJ5pa8ao3aO+MmlFKzJC1u/b8D8z2Lu0J+Vwe7qC:pPWrpU+5Rao3/LmuzJCM/bzgAz
MD5:	35639C3C895B57D5E4B5F764ABE5D940
SHA1:	269D5DE5F01924ADF9665A9F4D163EA553794BAA
SHA-256:	EA18037D4EB9771263CCA340B2AD31DA0CA807DAE7CDF8FD437266A853DE3D00
SHA-512:	6EB07EF59332D95985DA086B8FC1CA8A762D31CC6FCC14418C736CF211FB5B06381F876BF77C334C7140800BA5DBDEB1EAF07A401E47F0C4ABDEAD2D836389 2
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkJLx.img&ehk=ab4NFwKPiOUcoMjMzCCRK%2fouai5ROn4RlXwrt3nrHLY%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....L..]..:0..!t3<.....?x}k....tEgv..")ff'.....s.....Q..=...S....W.z....x.....X.....}..Z.....{}....\.....>....X(6i*.lbi..u[..P...O...y..E..l...%.:....Qwu.?...qz..u._ r.|.B.....M(..$.p...).9.z....zW.....[.....?C.m...dE..(.h.M.....v<..q..S6Yn...G.<....T.>V..|T.O]>.....-.....j.?L..X....S.@.H...L...P".Y..TT...~O..!..n....ecp.n..H...

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[4].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 144x144, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4662
Entropy (8bit):	7.906652539569635
Encrypted:	false
SSDEEP:	96:pPE9fuJsPbx60IPg+MMuPecZoXnNRLW/wG+fWRY:pPaf7bx6rg+7XnNRnGRY
MD5:	49A2DFF8082FCF50F4311C7867ECEDAD
SHA1:	A125B14C82BFB9A78C711C13CC479FDD1C9266EA
SHA-256:	442192ACEE743DBF8DBEC6A3BA8212AF4FDCFA1E08E96894168F11011176F525
SHA-512:	088A01E123048CB37238D611B7F01218EEDDF846FF42875AEDB756D91819B06A131ED272067E66C76C538112C14F676213D6EC5EA4B0D353B68E7BE056F0F08A
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkzlb.img&ehk=VW7SkyKxbL7LXUGh4v%2fSqtV2Ju%2b%2fdtlvyipIBuf1oQo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?....4..@.j.=AA9$....M..R.1..&...M#....:C..@..?.!.=i.A.j..-.....*.`...".".sH.)s.Oj.z...T.O4...N.....wz.6.....=.....@.....E .(.P.w.M'&.z.Zg.4.....Tc.g.L..ny. (.i.....C[..e.G...7{..Y.Ff.P...}.vvL..G....K.6.,.....a@..jve. .#"...c.m.8.X{.T..b..9....+..4X%?....Eq.v..N.L.#.....P.T..<W/.L...>e9..{..ja<.j3..,Py.. ...h.t..J8...~R=...i..v.0.4Ss..RP ..iI.R..9{.S..j^.CG

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[5].jpg

Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	6321
Entropy (8bit):	7.930428341817175
Encrypted:	false
SSDEEP:	96:pPEFWBYC3qBZJigkG/FdQS5zwu3LHBaWc4TUpz35BH7zQx5+FixuTKn7xF:pPGYYCaHsSdQSy8LHBaV4TU15tnQub2F
MD5:	AFF39E85868825504E8463C5CDD11BD7
SHA1:	DEF891B9A50BA0F8DA20DC93D5DFD80FFE330478
SHA-256:	17C3E9E4228BCBF6E56795D6D8539791483D4B1A07E4A542F32282D99C94FB75
SHA-512:	019D7C4382FEEC7EA3E7E26C20620327A9644A10AA13AEA9161C70DB8AAAD22BE452D4AF3D25E2C153C875BBA7D7C4B68D1EB2E128A212FB3E95C1F2568D9 B7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkGZS.img&ehk=QmtuVlo%2bL0J6PRmZTHf5eMhHSpsWN3gSG5N88RqgPWU%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..4._.]...O..X...k...^=.D.....k.m.H..$....C.kP[l,%.K.....G\....x..v....B.....?..uT....K.q.Kn".YV01.x.3A..O.I.a:.....R.!.#.e..YSqv{y....=y^...f.... ..W.Yx...!.d.....+..\....h.....S.L../X{.2..V...^.*q../Q[...f.....)...m..z..#.d.....v.~&.....#.V..A..z..W.i..O.B.HF2Y....T. ..FO..7....*G...xJ....r}.....;....';...P..N.G.R?..T.fq.....x

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\PSUEOSZZ\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5109
Entropy (8bit):	7.913384769447657
Encrypted:	false
SSDEEP:	96:pPELkaw+eKa2pvAJqZbK+VEYjHOxNtlurSUmBjQFr5i8T:pP0kaw+eKXfG+VEYyx1eSUmBI5/T
MD5:	27368154F2C3CF4EDEBC0A95CED35B43
SHA1:	5CAE3ECA10C9A32BC77AF7AEE1E2944590B8BD37
SHA-256:	4406423DC5F852B966777DE5272126839793C96251AB2F063A099C347BE396D9
SHA-512:	8313894648ADD4EF180464FA901403AB911B67A256DE09ACA665D66BA9EAEAE62A67624C3985F3E22BE537E4E8764FD32BD85C06BE7C3CD37A2418FDAD963EC
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fk2g2.img&ehk=6LEOa661FEfcyTEYPdN22SbtYfGFBqG3UnhDMs6fDjo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...<V>.....I..y5..t.z.K.Z.o.8.Y....]N.e"^Jv....:.+..$K..m..v.}..v./0R._j.....w.?...=.0.g.E>`..>...P>.Gc]..3.mb=.....Jq..M.H=k.k..B.dg.8.N.....3o .]..*z.P..?.O.9N(...M7i...}..v.}...|..9z+.}.....b;Q..cQZm.7....X...X.....1.c..IIK..k...b3.k.x..N{5q..|.\.:1.5Y.eQ..\.'...&..~.O+..9u.{…a].....|:.8Z,3.....C..I.....[z..V.-...Q.....x.....Y.g..q....mN.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\6sxhavkE4_SZHA_K4rwWmg67vF0.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines
Category:	downloaded
Size (bytes):	20320
Entropy (8bit):	5.35616705330287
Encrypted:	false
SSDEEP:	384:Kh4xTJXiXZ4sb4ZENXjTDDoFWZ3BnqIfP5IDV6s4RKAvKXAL5Nuwbv++9O:YoTdiJpjBpBnqIH+Z6se4XALueO
MD5:	07F6B49331D0BD13597934A20FAC385B
SHA1:	B39E1439D7FC072AF4961D4AB6DE07D0BC64B986
SHA-256:	4752E030AC235C73E92EC8BBF124D9A32A424457CA9A6D6027A9595DA76F98D7
SHA-512:	333B12B6BC7F72156026829E820A4F24759E15973B474E2FFB264DEE4C50B0E478128255E416F3194E8C170A28DF02AA425D720CC5E15BC2382EA2D6D57A6F5B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/6sxhavkE4_SZHA_K4rwWmg67vF0.gz.js
Preview:	/*!DisableJavascriptProfiler*/.var BM=BM||{};BM.config={B:{timeout:250,delay:750,maxUrlLength:300,sendlimit:20,maxPayloadSize:14e3},V:{distance:20},N:{maxUrlLength:300},E:{buffer:30,timeout:5e3,maxUrlLength:300},C:{distance:10}},function(n){function vt(){if(!document.querySelector||!document.querySelectorAll){k({FN:"init",S:"QuerySelector"});return}w={};e=[];ft=1;ut=0;rt=0;o=[];s=0;h=!1;var n=Math.floor(Math.random()*1e4).toString(36);t={P:{C:0,N:0,I:n,S:fi,M:r,T:0,K:r,F:0}};vi()}function ei(n,t){var r={};for(var i in n)i.indexOf("_")!==0&&(i in t&&(n[i]!==t[i]||i==="i")?(r[i]=t[i],n[i]=t[i]):r[i]=null);return r}function oi(n){var i={};for(var t in n)n.hasOwnProperty(t)&&(i[t]=n[t]);return i}function b(n,t,r,u){if(!h){k({FN:"snapshot",S:n});return}r=r||gt;t=t||!1;var f=g()+r;ot(o,n)===-1&&o.push(n);t?(yt(),pt(t,u)):f>s&&(yt(),rt=sb_st(pt,r),s=f)}function k(n){var u={T:"CI.BoxModelError",FID:"CI",Name:ht,SV:ct,P:t&&"P"in t?d(t.P):r,TS:f(),ST:v},i,e;for(i in n)u[i]=n[i];e=d(u);wt(e)}func

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\JDHEvZVDnqsG9UcxzgIdtGb6thw.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	408
Entropy (8bit):	5.040387533075148
Encrypted:	false
SSDEEP:	12:2QWV6yRZ1nkDXAn357CXYX0cO2mAICL2b3TRn:2QO6P+5OYXJPi3TRn
MD5:	B4D53E840DB74C55CC3E3E6B44C3DAC1
SHA1:	89616D8595CF2D26B581287239AFB62655426315
SHA-256:	622B88D7D03DDACC92B81FE80A30B3D5A04072268BF9473BB29621E884AAB5F6
SHA-512:	4798E4E1E907EAE161E67B9BAB42206CE0F22530871EEC63582161E29DD00D2D7034E7D12CB3FE56FFF673BC9BB01F0646F9CA5DAED288134CB25978EFBBECF
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/JDHEvZVDnqsG9UcxzgIdtGb6thw.gz.js
Preview:	(function(){function u(){n&&(n.value.length>0?Lib.CssClass.add(sj_b,t):Lib.CssClass.remove(sj_b,t))}function f(r){n.value="";Lib.CssClass.remove(sj_b,t);sj_log("CI.XButton","Clicked","1");i&&Lib.CssClass.add(i,"b_focus");n.focus();n.click();r&&(r.preventDefault(),r.stopPropagation())}var i=_ge("b_header"),n=_ge("sb_form_q"),r=_ge("sb_clt"),t="b_sbText";n&&r&&(sj_be(r,"click",f),sj_be(n,"keyup",u),u())})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\MDr1f9aJs4rBVf1F5DAtlALvweY.gz[1].js	
Size (bytes):	257
Entropy (8bit):	4.781091704776374
Encrypted:	false
SSDEEP:	3:qMH4WXMHwmnIB4JmhyfAIB4Jmml0X2IUJIB4JrNOsK1A4JWW7jKYHVA4JRGYdA4S:q6XzD4jr43ldI74FNQlNj7jM9TlMlbSr
MD5:	51A9EA95D5ED461ED98AC3D23A66AA15
SHA1:	62FBB857B873BD79BEE7F16D0766A452FA2798A3
SHA-256:	A5B4181611E951FAECD6C164D704569C633E95FE68D3D1934B911A089EBF70E8
SHA-512:	CEE4231894F82627E50EC746D7C150E5303A1BF8864D7B084173B9D17663A27CC2915F5D0D4DC0602FE26D9EAA10DD98CF3422E7601F520EF34D45C9A506D6F
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/MDr1f9aJs4rBVf1F5DAtlALvweY.gz.js
Preview:	var BM=BM||{};BM.rules={"#sc_hdu":[-1,-1,1],"#hp_id_hdr":[-1,-1,1],"#hp_container":[-1,-1,1],".hp_sw_logo":[-1,-1,0],".b_searchboxForm":[-1,-1,0],"#crs_pane":[-1,-1,0],"#sb_foot":[-1,-1,0],"#sh_rdiv":[-1,-1,0],"img,div[data-src]":[-1,-1,0],iframe:[-1,-1,0]}

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\RXZtj0lYpFm5XDPMpuGSsNG8i9I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	1220
Entropy (8bit):	5.024732410536042
Encrypted:	false
SSDEEP:	24:6Vj1V5FrGj6BBEEo6maDU6CWi4dDRRE0Slc7qHy5++vY:8v5TBG6U6C+DLSiL+P
MD5:	E34F2CDADA9986F52CCFAB129645ABAC
SHA1:	93FF6CA74EB48A6825F9BC21BEE52159987C0A82
SHA-256:	79C181E7D29CF735AE99FD86C42934D7FD6FB51E6481D788E1CB812C7DC63DF6
SHA-512:	671EF1DB12BEE74E8E6BAEE8850F4F6A278E51F2236A851A24D889CE40040273088B2D206F2AA42BD1475F4F88F7B4420BC4CE6922023DE205308C56A3C96A4C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/RXZtj0lYpFm5XDPMpuGSsNG8i9I.gz.js
Preview:	var Feedback;(function(n){var t;(function(){"use strict";function u(t,i){var u=t.getAttribute("id"),f;u||(u="genId"+n.length,t.setAttribute("id",u));f=new r(u,i,t.getAttribute(i));n.push(f)}function i(n,t,i){i===null?n.removeAttribute(t):n.setAttribute(t,i)}function t(n,t,r,f){for(var e,s=_d.querySelectorAll(r),o=0;o<s.length;o++)(e=s[o],f&&e.id&&f[e.id])||(u(e,n),i(e,n,t))}function f(n){for(var u=_d.querySelectorAll(n),e=1,f={},t,i,r=0;r<u.length;++r){if(t=u[r],!t.id){for(;;)if(i="fbpgdgelem"+e++,!_ge(i))break;t.id=i}f[t.id]=t}return f}function e(){var i="tabindex",r="-1",n=f("#fbpgdg, #fbpgdg *");t(i,r,"div",n);t(i,r,"svg",n);t(i,r,"a",n);t(i,r,"li",n);t(i,r,"input",n);t(i,r,"select",n);t("aria-hidden","true","body :not(script):not(style)",n)}function o(){for(var r,t=0;t<n.length;t++)r=_d.getElementById(n[t].id),r&&i(r,n[t].attributeName,n[t].originalAttributeValue);n.length=0}function s(){typeof sj_evt!="undefined"&&(sj_evt.bind("onFeedbackStarting",function(){e()}),sj_evt.bind("onF

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\a282eRIAnHsW_URoyogdzsukm_o.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	423
Entropy (8bit):	5.117319003552808
Encrypted:	false
SSDEEP:	12:2gSYjthM4GF4aaXtdhI9DfaUZnsMQYAQI:2gSW/bS9/ZnsMAj
MD5:	3A5049DB26AF9CE03DB6A53D3541082D
SHA1:	934DAEA4EDDE2568CA02AB89AF23FDCFEB57339A
SHA-256:	AF8C36DEFED55D79106513865F69933E546E1E4C361E41C29F65905DED009047
SHA-512:	5E21B6E184CBB0013DCCE174345DAC14BB64D391CCA3B253F73C7373253FDCA5E0BB297A0BD2FAD237E4F796895807660369680621C49C8F99DF428ED3218C9
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/a282eRIAnHsW_URoyogdzsukm_o.gz.js
Preview:	(function(n){function i(){var e,o,u,s,f,r;if(document.querySelector&&document.querySelectorAll){e=[];o=n.rules;for(u in o)for(s=o[u],u+=!s[2]?"":" >*",f=document.querySelectorAll(u),r=0;r<f.length;r++){var i=f[r],h=0,c=0,l=i.offsetWidth,a=i.offsetHeight;do h+=i.offsetLeft,c+=i.offsetTop;while(i=i.offsetParent);e.push({_e:f[r],x:h,y:c,w:l,h:a})}n.enqueue(t,e)}}var t="L";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	PNG image data, 15 x 15, 8-bit colormap, non-interlaced
Category:	downloaded
Size (bytes):	748
Entropy (8bit):	7.249606135668305
Encrypted:	false
SSDEEP:	12:6v/7/2QeZ7HVJ6o6yiq1p4tSQfAVFcm6R2HkZuU4fB4CsY4NJlrvMezoW2uONroc:GeZ6oLiqkbDuU4fqzTrvMeBBlE
MD5:	C4F558C4C8B56858F15C09037CD6625A
SHA1:	EE497CC061D6A7A59BB66DEFEA65F9A8145BA240
SHA-256:	39E7DE847C9F731EAA72338AD9053217B957859DE27B50B6474EC42971530781
SHA-512:	D60353D3FBEA2992D96795BA30B20727B022B9164B2094B922921D33CA7CE1634713693AC191F8F5708954544F7648F4840BCD5B62CB6A032EF292A8B0E52A44

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\down[1]	
Malicious:	false
IE Cache URL:	res://ieframe.dll/down.png
Preview:	.PNG.....IHDR.....ex....PLTE....W..W..W..W..W..W..W..W..W..W..W..W..W..W.U.....W..W.!Y.#Z.$\.'].<r.=s.P..Q..Q..U..o..p..r..x..z..~..... ....b.....$..s...7tRNS.a.o(,.s....e.....q*..... .....F.Z....IDATx^%.S..@.C..jm.mTk...m.?|;.y..S....F.t...,.....D.>..LpX=f.M...H4.....=...=..xy.[h..7....7.....<.q.kH....#+....l..z.....'.ksC...X<.+..J>....%3BmqaV ...h..Z._.:<.Y_jG...vN^.<>.Nu.u@.....M....?...1D.m~)s8..&....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with no line terminators
Category:	downloaded
Size (bytes):	229
Entropy (8bit):	4.773871204083538
Encrypted:	false
SSDEEP:	3:2LGffIc6CaA5FSAGG4Aj6NhyII6RwZtSAnM+LAX6jUYkjdnwO6yJxWbMPJ/WrE6J:2LGXX6wFSADj6iIunnyh6TbMFsise2
MD5:	EEE26AAC05916E789B25E56157B2C712
SHA1:	5B35C3F44331CC91FC4BAB7D2D710C90E538BC8B
SHA-256:	249BCDCAA655BDEE9D61EDFF9D93544FA343E0C2B4DCA4EC4264AF2CB00216C2
SHA-512:	A664F5A91230C0715758416ADACEEAEFDC9E1A567A20A2331A476A82E08DF7268914DA2F085846A744B073011FD36B1FB47B8E4EED3A0C9F908790439C930538
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eRYlUYIMYsB_Pt8B7FTik-pl5cs.gz.js
Preview:	(function(){var t=_ge("id_h"),n=_ge("langChange"),i=_ge("me_header"),r=_ge("langDId"),u=_ge("mapContainer");t!=null&&n!=null&&i==null&&(r===null||u===null)&&(t. insertBefore(n,t.firstChild),n.className=n.className+" langdisp")})()

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\eaMqCdNxIXjLc0ATep7tsFkfmSA.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	2678
Entropy (8bit):	5.2826483006453255
Encrypted:	false
SSDEEP:	48:5sksiMwg1S0h195DlYt/5ZS/wAtKciZIgDa4V8ahSuf/Z/92zBDZDNJC0x0M:yklg1zbed3SBkdZYcZGVFNJCRM
MD5:	270D1E6437F036799637F0E1DFBDCAB5
SHA1:	5EDC39E2B6B1EF946F200282023DEDA21AC22DDE
SHA-256:	783AC9FA4590EB0F713A5BCB1E402A1CB0EE32BB06B3C7558043D9459F47956E
SHA-512:	10A5CE856D909C5C6618DE662DF1C21FA515D8B508938898E4EE64A70B61BE5F219F50917E4605BB57DB6825C925D37F01695A08A01A3C58E5194268B2F4DB3D
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/eaMqCdNxIXjLc0ATep7tsFkfmSA.gz.js

Preview:	var IPv6Tests;(function(n){function c(t){var r,c,o,l,f,s,i,a,v;try{if(y(),t==null||t.length==0)return;if(r=sj_cook.get(n.ipv6testcookie,n.ipv6testcrumb),r!=null&&r=="1"&&!u)return;
	if(c=sj_cook.get(n.ipv6testcookie,n.iptypecrumb),r!=null&&c&&u&&(o=Number(r),l=(new Date).getTime(),o!=NaN&&o>l))return;if(f=_d.getElementsByTagName("head")[0],
	!f)return;if(s="ipV6TestScript"+t,i=sj_ce("script",s),i.type="text/javascript",i.async=!0,i.onerror=function(){Log.Log("ipv6test","IPv6Test Dom_ "+t,"IPv6TestError",!1,"E
	rror","JSONP call resulted in error.")},a=_ge(s),a&&f)return;f.insertBefore(i,f.firstChild);i.setAttribute("src",_w.location.protocol+"//"+t+".bing.com/ipv6test/test");e&&p();v=u?(
	new Date).getTime()+h:"1";sj_cook.set(n.ipv6testcookie,n.ipv6testcrumb,v.toString(),!1)}catch(w){Log.Log("ipv6test","Dom_ "+t,"IPv6TestError",!1,"Error","Failed to make J
	SONP call. Exception - "+w.message)}}function l(t){if(!t){Log.Log("ipv6test","IPv6TestResponseError","IPv6TestError",!1,"Error","Got null re

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\hceflue5sqxkKta9dP3R-IFtPuY.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	426
Entropy (8bit):	4.904019517984965
Encrypted:	false
SSDEEP:	12:2gcmRRt9Y4LF1Zd4XV4LFUXCdg/qUWYzP++xAQI:2gcmRRFfgiUb6MAj
MD5:	857A0DE0BBF14F3427A1AFA5CD985BCE
SHA1:	0C1D2E767F07E5C0F14EA64980DB213D379CC6F7
SHA-256:	3ED65F33193430C0B9DB61FFE7F5FE27B29F86A28563992C3AFC47D4C22C23D7
SHA-512:	E7F2603855A16464417B772517676F080CCEFFB8069C687BAC798B7EB2875FCDC207E40E8C56E7CFFD4D56CED572270988599D1D2B73FB8AAA7FDD076FE3E7E 7
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/hceflue5sqxkKta9dP3R-IFtPuY.gz.js
Preview:	(function(n){function i(){var i=document.documentElement,r=document.body,u="innerWidth"in window?window.innerWidth:i.clientWidth,f="innerHeight"in window?window .innerHeight:i.clientHeight,e=window.pageXOffset||i.scrollLeft,o=window.pageYOffset||i.scrollTop,s=document.visibilityState||"default";n.enqueue(t,{x:e,y:o,w:u,h:f,dw:r.c lientWidth,dh:r.clientHeight,v:s})}var t="V";n.wireup(t,{load:null,compute:i,unload:null})})(BM)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\httpErrorPagesScripts[1]	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	12105
Entropy (8bit):	5.451485481468043
Encrypted:	false
SSDEEP:	192:x20iniOciwd1BtvjrG8tAGGGVWnvyJVUrUiki3ayimi5ezLCvJG1gwm3z:xPini/i+1Btvjy815ZVUwiki3ayimi5f
MD5:	9234071287E637F85D721463C488704C
SHA1:	CCA09B1E0FBA38BA29D3972ED8DCECEFDEF8C152
SHA-256:	65CC039890C7CEB927CE40F6F199D74E49B8058C3F8A6E22E8F916AD90EA8649
SHA-512:	87D691987E7A2F69AD8605F35F94241AB7E68AD4F55AD384F1F0D40DC59FFD1432C758123661EE39443D624C881B01DCD228A67AFB8700FE5E66FC794A6C0384
Malicious:	false
Preview:	...function isExternalUrlSafeForNavigation(urlStr)..{..var regEx = new RegExp("^(http(s?)|ftp|file)://", "i");..return regEx.exec(urlStr);..}..function clickRefresh()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..window.location.replace(location.substring(poundIndex+1));..}..}..function navCancelInit()..{..var location = window.location.href;..var poundIndex = location.indexOf('#');..if (poundIndex != -1 && poundIndex+1 < location.length && isExternalUrlSafeForNavigation(location.substring(poundIndex+1)))..{..var bElement = document.createElement("A");..bElement.innerText = L_REFRESH_TEXT;..bElement.href = 'javascript:clickRefresh()';..navCancelContainer.appendChild(bElement);..}..else..{..var textNode = document.createTextNode(L_RELOAD_TEXT);..navCancelContainer.appendChild(textNode);..}..}..function getDisplayValue(elem

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sTWC0LplwPyIP_jw8VjHps800ZQ.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	16386
Entropy (8bit):	5.2866519663601315
Encrypted:	false
SSDEEP:	384:+WLj/9N/zdUjP+c4QQKaK9JASETkyWJLhjO4YuiqRqNlRxW+:+u/P/zdUraOJhaShK1uiqR0T3
MD5:	44AD44162E25A1DB1F46F78B8ECFAD42
SHA1:	C63A0E7B132221D572A541F700601356627A98A4
SHA-256:	5AE500A4737BE7B187EEA99AAB81CF3D4796D23550F7C5349DE2430E6624918D
SHA-512:	4F0078431E86CCD8C0B3DE7E4F7CC10B184DC5376AD10C224EC081DAE1B9D16509E01A95CE3F3B4F7C394EC2C52782E4CB9AC2DE8C12CA0FFC9CC66C01C5AFD
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/sTWC0LplwPyIP_jw8VjHps800ZQ.gz.js
Preview:	var customEvents,__spreadArrays,fallbackReplay,EventLoggingModule;_w.EventsToDuplicate=[];_w.useSharedLocalStorage=!1;define("shared",["require","exports"],function(n,t){function s(n,t){for(var r=n.length,i=0;i<r;i++)t(n[i])}function r(n){for(var i=[],t=1;t<arguments.length;t++)i[t-1]=arguments[t];return function(){n.apply(null,i)}}function u(n){i&&event&&(event.returnValue=!1);n&&typeof n.preventDefault=="function"&&n.preventDefault()}function f(n){i&&event&&(event.cancelBubble=!0);n&&typeof n.stopPropagation=="function"&&n.stopPropagation()}function e(n,t,i){for(var r=0;n&&n.offsetParent&&n!=(i||document.body);)r+=n["offset"+t],n=n.offsetParent;return r}function o(){return(new Date).getTime()}function h(n){return i?event:n}function c(n){return i?event?event.srcElement:null:n.target}function l(n){return i?event?event.fromElement:null:n.relatedTarget}function a(n){return i?event?event.toElement:null:n.relatedTarget}function v(n,t,i){while(n&&n!=(i||document.body)){if(n==t)return!0;n=n.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\sjm7ZxOOdUKgLq2Lulikx_Lt20I.gz[1].js	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	exported SGML document, ASCII text, with very long lines, with no line terminators
Category:	downloaded
Size (bytes):	4623
Entropy (8bit):	5.164231565021591
Encrypted:	false
SSDEEP:	96:B3D+ca6IQkQQX6hJmK/Vl3A2zLEzvPTkyfXeJLYryYHIZq76/PH:V+ca6IBQQX6aK9l3ASivPTkyWJLh7R
MD5:	8FD5ED5E0730854741D73A66E1C8C124
SHA1:	8A4D348BA92FEBAB3A5FC7FFDED98E0841C3CE9C
SHA-256:	63C3206CB8509C0A2DD25A0AA3555BD49E7B2E24AE95F6CB7E6521D830C986F7
SHA-512:	D52D1CCBBEDDC49B850030E3B2ABA9EADE824AE74EF4FF7055D50EDDCABC7933D6D662FEE8DF0F37B20F096E96908DA0CB89FF8DFC4E6AB14F1255BBDE745A40
Malicious:	false
IE Cache URL:	http://https://www.bing.com/rp/sjm7ZxOOdUKgLq2Lulikx_Lt20I.gz.js
Preview:	define("rmsajax",["require","exports"],function(n,t){function c(){for(var i,n=[],t=0;t<arguments.length;t++)n[t]=arguments[t];if(n.length!=0){if(i=n[n.length-1],n.length==1)ot(i)&&f.push(i);else if(n.length==3){var o=n[0],s=n[1],u=n[2];st(o)&&st(s)&&ot(u)&&(ht(r,o,u),ht(e,s,u))}return window.rms}}function nt(){var i=arguments,n,t;for(o.push(i),n=0;n<i.length;n++)t=i[n],ct(t,r),t.d&&tt.call(null,t);return window.rms}function kt(){var t=arguments,n;for(s.push(t),n=0;n<t.length;n++)ct(t[n],e);return window.rms}function l(){var t,i,n;for(ri(),t=!1,n=0;n<o.length;n++)t=tt.apply(null,p.call(o[n],0))||t;for(i=0;i<s.length;i++)t=ti.apply(null,p.call(s[i],0))||t;if(!t)for(n=0;n<f.length;n++)f[n]()}function tt(){var n=arguments,t,i,f,e;if(n.length===0)return!1;if(t=r[ut(n[0])],n.length>1)for(i=ui.apply(null,n),f=0;f<i.length;f++)e=i[f],e.run=u,dt(e,function(n){return function(){gt(n,i)}}(e));else t.run=u,ft(t,function(){it(t)});return!0}function dt(n,t){var f,u,r;if(!n.state){if(n.state=pt,at(n)

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[1].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 72x72, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[1].jpg	
Size (bytes):	6060
Entropy (8bit):	7.899886568977212
Encrypted:	false
SSDEEP:	96:5PEDuvFap14aVq/0qYmgFTM1tprjZ9bbO5/X0grBaziE8fTiC+Y6LmlBuhL7kABa:5PsuvFa34aU/0+4M1LrlFChEoBaziE8t
MD5:	92B5E4056C43E152A909428A855A992C
SHA1:	0C7F041BE81D39FAA31CBD8CA0037AC27B204262
SHA-256:	FFC09BE491D6A9BD2B7BD02AF00ECD82A21F0D8E00536D7E131AAF1BAF67F945
SHA-512:	B88EC4567BC00DA4DEBAA3054D0CF9724E7E9E616A83EB8AB8D685E2EDB119BF695AE537A9A5763487A4A85D24BC9A308A682A611DAA8D41EF56D84722B25C A0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flpDy.img&ehk=pFN%2bVPGNJ3ndWfb%2b8%2f%2bj2d0fgzq8df%2bWLedXMSOU4fo%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....H.H.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?..Fs..Z.(.8...P]gO:|..w.[.....a.&.h^!..l!.i.+.Q.B.....[.l..L..4q..."DM.....qY.;Ci.Z.j?l....F...<._..[.V..6..[=...@X.....j..*....y`....Q....=I....k..Iwx.")*...n.S.{W.j.$...I...F...,#m.....IDj7=.....&.c.....)...V.i .. ...I*.&...4+..0.4....=.....o.=..c..N..f.Y.....).....k.G...[..4....`.O8#....!...'57tM.<P.(.5@.....J....=(....2.:P.m...../.....R..P...c.C=.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[2].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5777
Entropy (8bit):	7.917920871216737
Encrypted:	false
SSDEEP:	96:pPEQBGjpz1df7dAJrDp5OiC9PchAeKBc9VSwpCcGpZcU1DwGO1pHRsKdDcn:pPTBGjlrf7dNchnrCnZcUwG4Rldon
MD5:	7D10F16EA455E49470853BE05415E27E
SHA1:	0370FE7D24274A9A5909355C042EBBF9E795FD85
SHA-256:	1DB14FB96D4E49265DEFB60E98BD6C39A2724B1EBC21D50E0F2E60F3859EE93A
SHA-512:	DF233159BC504BA5C8D8759AE631A2D5CE9AB48060EDC84EEF2674749AEE1D5E0A3B5BD5AE8EF3F54FDFBBD1F7FE0B9D26FD1FC99593DAC78396EE2209CE1 B0C
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1flksC.img&ehk=H0FCoWHkkRHx9dwEmzqiKOqgx9bfKAuVCxCQfuDoLvw%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?.....;@..^H[~O.=..l.5.s.....8.....%'=..Hd.q..?.W'..... .;..J$...=.E$.P1.h../..7.z.....ZxF....f1...R.~...i\v!..... .>...u!...9.....\<.I..A....8.....#....-.....h. .|.#tcV..e....1Q.A..W].qV..*..B.i$.z7...Kz.(..l7.#....T?3...o7..H..c(..O..qYF-d.w.\.#.P...y..Hn&~J.S.c5j..6..c....b...N6.L..F.=..M.(.dw..2....f.ce;GC..W*.x|.....*5....4....v!.c.t 4.+7.9.5".J

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[3].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4987
Entropy (8bit):	7.9205495681055185
Encrypted:	false
SSDEEP:	96:pPE32PK2X6035EzsdUWfNwjh4D8+MhUb80LvFwJp:pPi2PK2Xf35ljWfA4D24LFwH
MD5:	E8349E3EA51D3A6E24284176981359EA
SHA1:	0E009269A3DC197C7C46B765D24AC1F531AA4810
SHA-256:	D88B8253842FB58AADAAEA2166863ADBFF91B77F0CAD8501100A47B7B9A999F6
SHA-512:	85B79D9B4B2C47415EBD2E710EC71B66496F09BDB8822CF8AF7453C3C9D9423869FE3B4DD4D31A89ECFD7E7BC72A55205A306296369F490C12FB05800B6A2A0
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkU9t.img&ehk=mxhBThhQVDlo%2bCYW2VhueyqJguPlSKZ1mWMM3nr17PY%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====..."}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.....?...i.....h..f....E.:.m-..h.74.....I.n.FE...f..I...;4..f.u.<.Bi.....LQLE.Z..U..A.$zS..|8..W(....e.e.F....;F..4.....H..9..;..-q...G.0...]...i....k.....RI.\F.{...G s ...K1..2I8.U;.f.L.....X"iLK'....H..s.....%.H....O..q..G].7.n.$X.pcE...A....k..YS.Kfz8L,+...E+...#....%.D1.....G.+..&.(...\..\.w=C.@.....er.D"h...Fs.J..%.i.s.....:.8. ..i..1.....=k.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[4].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[4].jpg	
Category:	downloaded
Size (bytes):	3726
Entropy (8bit):	7.864083694829938
Encrypted:	false
SSDEEP:	48:pyYcuERAB4Zyb8BrwdM18WIaMAVwIIjMC+FrFza8JmQOQYBhvSp/BSq/DVimjw:pPEZc8ROMWWLMcj7rFza8/VY4MsVij
MD5:	A6E6FD3AB66E5A2F49A45CCB2B61B19D
SHA1:	9A7EC1C26991AFC76B694BECB95639DDE2AB9DA2
SHA-256:	8FB3DE41169B7B8547E4F07836C9C9503655B613678E58DE449A0CB65DFACCE4
SHA-512:	278DD1A867D863F595FB3B8398399F5EAFC332FB29981EF4BF9B14DBCBFBC55A9AC2CE3A86EB4A95F6CFC8C8BE9B60FF690BF9AB436D2AD270A3981ED23B4 7B
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkXNm.img&ehk=kxyU8xKPJMs4tMRWRT6cTgj6Bfiij4nG3t8YLJw8HCQ%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....i....Q..@...P.c....8..;..*..\.@.>.....+.:iV.c.0.D.ub.j._..7.G....f.$(..p2....MsN..b..3+tBy>.Z.O.h. .e.O..e....n +._g....p.{....x.f..o,<^...g.\>....7P.* R..#..b0kB..%%tq.....Q@..Q@...u!...(...R.v(..KE.....{....H'.....U,!X.2....K.sa2...p.W8..s...GL...Q./0v.2..$q...q..Gv.....!.r...IU..._U....AYZFn.H^=I=.e..B.+\l4..I.y..p@...j..... A...M.+.v:lG.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[5].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 300x300, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	4579
Entropy (8bit):	7.899738415633208
Encrypted:	false
SSDEEP:	96:pPElQIszgVi+8yJg1On37lfYKgsaU4AzO/wVie:pPk50gd8ysW5QKgizce
MD5:	6252E142AFB55FA1C5DD093059E5B784
SHA1:	FA2DEDFB97B7BF7B2D1052EA4B0DEC214E4217A1
SHA-256:	24461B5094C1DC8AA9F6741AD78006FF35954478933E003E2CD036EA8E303EA4
SHA-512:	A6156F1C962CE251B79C86F5A5B5BBA8C3D8C1060251CD69365C650D5BF2480ED14A6F36CFF4235BB0E53DC15903086CF901891B2DEEC050271A851D88C3DE
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fket7.img&ehk=x1iCxRdz8nKwKjWtFCBaxEx1tovE7Q0NcYc3bmTeH%2fl%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....,.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..f..$H.."(.f'..rk..9.....B<...9.c.:...E,.....=...w.....,_h.....yttW=.....tr..>l0..+.fE.,z..s..js.....5,.....i.....+.Cm=.3Sj.6.|.r...>.G.....W.Z.]){..i[..&.C...,.*A. ..s.u.....s.S.>ni..t.;....OH..i.3N.R.[..2..7..*.#.}SP..O.X@.....zt98.YzR..2..9.`Y..r..ZN.,..+9Tp.....C.cS.>.PT..X.....S..8S..moJV..<.>..Z.U.).7ZV..!..h.0.S.\..eX5k)..Gp.O....J..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\WJ8I2OL4\th[6].jpg	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 150x150, frames 3
Category:	downloaded
Size (bytes):	5718
Entropy (8bit):	7.9318718460651025
Encrypted:	false
SSDEEP:	96:pPEJOqsYH47+dCCG6wRGFkXNcO8XOnW81LsImKDFLMwLXZUIEAWgKhE1:pPeOKH470Cv6wRGFSGO8kZ1L8+oiZUrg
MD5:	5ABBBE53C535080AE3BE91FE6F0B93C1
SHA1:	6A991409D0A6886057BBD0DC9AE71AAFB111E8C1
SHA-256:	B692C27DDDA4FFE62BB2C57AA229EB9298EBDA7726BC227089CEEFDF5E05AD4C
SHA-512:	2283634663D24B2C87399A5C562C5E73C68905BF799FD41367D15E4BCF336B5BA5511706998D9C439016799E56B20E5693BCCECA1D9037223D07659410570EC6
Malicious:	false
IE Cache URL:	http://https://www.bing.com/th?u=https%3a%2f%2fimg-s-msn-com.akamaized.net%2ftenant%2famp%2fentityid%2fBB1fkfuX.img&ehk=Al75D9k%2bIhZGZEnhR9bRctnjlt4TfOCoHOzqmGEyQNE%3d&w=150&h=150&c=8&rs=2&pid=WP0
Preview:	......JFIF.....`.`.....C.....$ &%# #"(-90(*6+"#2D26;=@@@&0FKE>J9?@=...C.....=)#)=====.. .....".....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?..5..Z...9.{...<....[w..G..W7;.....P.-%V.c..L.>....`A..5.i.".i..A.<.k.....^.Z..u.....8.....&.9.I.....&..\l.>Ty(.xs...b.....U.*id...r....}zV...Xk>cm.*.[..5.(. u.F.....P....;.x....{c..mxfR.....fk....;>..]....[H.u.eO.....4<..C..m.a.....J`..c...z....-.`.B.._S._....!.....l9.N1...PZ.....z.N...)...M~/.i.p.y.H.b.xP}Y....k.....4.X]).l.Fb

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Process:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
File Type:	ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\JavaDeployReg.log	
Category:	modified
Size (bytes):	89
Entropy (8bit):	4.496494847193787
Encrypted:	false
SSDEEP:	3:oVXU15FdT5dzdR98JOGXnE15FdT5dzS+n:o9U7Fd39qE7Fdt
MD5:	C5768BEEAE31AEBFA92FB993771F9B50
SHA1:	1E6984D7A43E4A59919330711F787AD0C24F1A72
SHA-256:	130460A32AACC77F28393C9256180ADC58B26A77E22A18C3D7A6791603E0DC44
SHA-512:	F668D539DD5B593A3DA04B6D13EAF9077EA5351E5130511441AA40C6B9AA63FD88BD2673DD4934CE2C194B26D06DFB1A4C54ABFB3F0DB329E5BB21C10DE4F 76
Malicious:	false
Preview:	[2021/04/06 09:56:48.640] Latest deploy version: ..[2021/04/06 09:56:48.640] 11.211.2 ..

C:\Users\user\AppData\Local\Temp\~DF0368A8A894E8950F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39601
Entropy (8bit):	0.5639195295857624
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+8aAhKE6WmtjWo6WmtjWI6WmtjWZ:kBqoxKAuqR+8aAhKEjmtjjjmtjHjmtjM
MD5:	F6F579084DE60328B7D242DFC7C4E699
SHA1:	E776FD72ECBF259B4141EFD5749D9968D4291021
SHA-256:	8C7384F8293D79F2C95809EE8999E8FE729EEE14C63B9ACA1CD87BDDA6C39D8D
SHA-512:	D18627F91C493B37F1174C353B27EF96F04ED14FB580B1A10FFADC780A5471307D91185B99DF4FE595286267E0602A679EB6A03146F1A61E5C198BFB3D4E5B8B
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF1CDCF234EEFCC970.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.6012197418597929
Encrypted:	false
SSDEEP:	24:c9lLh9lLh9lIn9lIn9loNGF9loNq9lWN7kOu3uhJkCwFuh4YuCwS:kBqoInB5kO4eYe/R
MD5:	D368A5420D70DD26A2DDBFAA7112ABDC
SHA1:	4FCA24846FEAC551BC4C22445E8D1E8DB6C566E9
SHA-256:	C12493FD18D4E9FD17E896FF537B1F7E73FE20AEB62590ACBC672E9B6B7C62FE
SHA-512:	1E108912A37A6E69F54F844DB629F282611E343BFFDBC855B8AA574EDBE7507B2BFA465B242082F0250272F4F3D2ABDA4DF816A91C6811B3DC1E06DF659A82F
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF429EC30D8A24338F.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.5977273918091236
Encrypted:	false
SSDEEP:	48:kBqoI969E9Sk+JCSk+6X+6R+zrk+6R+0F+0iCSre:kBqoI0qig0JTfTJ8v
MD5:	359991E8BAFF6D72B466512C268E0F26
SHA1:	D446517F59639E042482648FA81FDAE0BAACB516
SHA-256:	B0AE4304B8F4646A330A7D389D1AC5C3952295EF806AABBE425E49AC1D55BADD
SHA-512:	DC1C845077F1AF6D66BEDFF58909F030C17764AA7971F8BD435F04EADA81D18DD57EB4FC07B82A8F7AA357DF243E5702229DCD1703B52D117224494AE12DC4 0
Malicious:	false

C:\Users\user\AppData\Local\Temp\~DF429EC30D8A24338F.TMP	
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF4EC0ACC0598C2A74.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39577
Entropy (8bit):	0.5577818234941052
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+/V/7/5/o/r/1VGg8O4VGg8OsVGg8OF:kBqoxKAuqR+9DhAjdLILcL1
MD5:	843F1E96A2491EBABA81FD2B7E4D7EC3
SHA1:	5EE79A42C9B265ACD230DE6BA4B67F5D0C240F16
SHA-256:	5224171EB0747689181F44EC5A91BF6E9F3DD4EAF27ADEE598314068DE851F75
SHA-512:	9AFB693E494F59E8B682CA22AEDF04DC753ECFC9DC7B40B30FBE09884E506034D6395BC9BD0584F38971B361309DF834F5ED3E60732326C8490122B61DC8649
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9401D896BB639998.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	53506
Entropy (8bit):	1.1339945391888944
Encrypted:	false
SSDEEP:	384:kBqoxKAuqR+8aAhKQ1Xb4jlWgfiOfiRZfi8AobYa:vioiPi
MD5:	4F025A160EBF95AB5CFA42DF753D41EB
SHA1:	3AB02A53341C96E854238920F45EF70C1DC5BD73
SHA-256:	38856E071442A641985086461B132324F786A08F5DB4E38E04928F25A39F3F66
SHA-512:	1314A7DCB352C22601FB8DF34AF917F947EDE78D6B6EBCEEA17CFBD408FBF0DCB2AFB5671575FC2D70A9494CB7458C8F5A391BB336DB8C3613103595D1B378 C
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DF9C40D021B9977A72.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39601
Entropy (8bit):	0.5661740370033982
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS+AGcdGgOeHatgRn7qOeHatgRn7qOeHatgRn7T:kBqoxKAuqR+AGcdGg7Q7A7x
MD5:	DE6B7C72C5D813A2053482E4002E1875
SHA1:	90B76A4B4179B7FC75EE196AC393279D29EBB2B9
SHA-256:	B4B90C080EF6A0832EE2A1FA7244A98DADFE9CFAD5FDB14BA9AA01CC99E5CF13
SHA-512:	B6E20520B97294A9DC4BB5EB91FEB2C08C10E47D0350F9A30C858FFEBDF31DDA8494517AFE437625BCE2B85EF7D168C8F0DD7E00AAA3395F35B54B29409694 3
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFB5C248C8321BA21B.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	39601

C:\Users\user\AppData\Local\Temp\~DFB5C248C8321BA21B.TMP	
Entropy (8bit):	0.5641388426895527
Encrypted:	false
SSDEEP:	48:kBqoxKAuvScS+HVH7H5HoHEIHEuFEBcBfgV+eFEBcBfgV+OFEBcBfgV+H:kBqoxKAuvScS+1bZILhKcB8KcBsKcBN
MD5:	F9746A9685545235E0BA980D3528F92D
SHA1:	AD68B622032855C9CB43FFB1871549340335D863
SHA-256:	BFD954061BD3F1FB89D3613F856B001C8A5469BE8C77F649AADCDFE3132F2FB9
SHA-512:	5409581D77F29ABDB6051F60621DA2747DC8555FB85696EF98910B2B4A946BD56D30CB258A5E14C67E2CA79576BEB31C025B611800621DFAD5A07635749D73FA
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFE1DAC2358EB1BABD.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	50659
Entropy (8bit):	0.9201780504904888
Encrypted:	false
SSDEEP:	96:kBqoxKAuvScS++4y7oqZMRbfuRbfMCRbfcRbfiRbfpRbfj7T0MRbfxtyRbf/VRbf:kBqoxKAuqR++4y7oqscAMew73hlObz
MD5:	2C78BB9F3B0B8DD6BAEC110210B5327E
SHA1:	3D17DACF345A5A117E09F633926954BC5498D934
SHA-256:	6BDC35D6A61CB6231F2410501658B9E919BAB9BE5049B67B84450241C0C9D518
SHA-512:	E65F0D50F62FFDC67E0ECAD989791678C7A5245E870221AB2B56E8530505DFF09A5D7CE33C1172BAB099F603EE8D1A968C08C0CB1486D3E09257B0199D5D3DF
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

C:\Users\user\AppData\Local\Temp\~DFFD6D62BD380D5B9D.TMP	
Process:	C:\Program Files\internet explorer\iexplore.exe
File Type:	data
Category:	dropped
Size (bytes):	13237
Entropy (8bit):	0.6002404057791108
Encrypted:	false
SSDEEP:	192:kBqoIF+FgFyQp9QZIZO5KejQZOv4v/9jq:kBqoIg+o
MD5:	0B384CDAF7922641E866D9CE30D7A1B9
SHA1:	CD1F9985D2527CC2AAFCAA853A4C68C6056026D8
SHA-256:	1DB52E1C94AF2B8D11EA190DF273DB7840B3F4C79B157CC1891AE9F25A3C49C4
SHA-512:	C6B932DC0AAAFC82466CFF5837A61D5ECB84E2838A9913FFEED9366801A06CA4AE995E88880E9F717DD4F37E542B2ED482B30F6CC422AFB80948925785FF2C0 E
Malicious:	false
Preview:	............................*%..H..M..{y..+.0...(.................. ....*%..H..M..{y..+.0...(.................. ....

Static File Info

General

File type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.610226321483174
TrID:	• Win32 Dynamic Link Library (generic) (1002004/3) 99.60% • Generic Win/DOS Executable (2004/3) 0.20% • DOS Executable Generic (2002/1) 0.20% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	0204_1.gif.dll
File size:	112787

General

MD5:	6ebc18a521638630f9b89ddb23c13b22
SHA1:	6bf2fd63e47f2b278ef75cca3893d87855c646d6
SHA256:	65179a35467708828de13c9a53f254c956cc4235a0196e3c53ca5022c176a6aa
SHA512:	6d9de680afa776e8291a3cb05f7e4bbac934815a17ba4cc9be3405df1177e081cca5555382b5e1b45832bb9dc2d17dfaa7be01eeca8e25552600834d23d9f674
SSDEEP:	1536:DWKaY5Se9WnVI78XvnoxJasJvRHKmyGDvDk0Rt9Y56l5ZMpvV05o9OX5xPw8:DWa0eQnVI7qCqZGDvDk4wol5w0EU
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._W...6e..6e..6e..)v..6e...w..6e.Rich.6e.....PE..L.....f`.....I.....Z.....`.....p.....

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x10006099
Entrypoint Section:	.code
Digitally signed:	false
Imagebase:	0x10000000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, DLL
DLL Characteristics:	
Time Stamp:	0x6066E9D0 [Fri Apr 2 09:54:24 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	811de8e945c2087a6e052096546cd842

Entrypoint Preview

Instruction
push ebx
push ebx
and dword ptr [esp], 00000000h
add dword ptr [esp], ebp
mov ebp, esp
add esp, FFFFFFF8h
push esi
mov dword ptr [esp], FFFF0000h
call 00007F0F90A30310h
push ecx
add dword ptr [esp], 00000247h
sub dword ptr [esp], ecx
push ecx
mov dword ptr [esp], 00005267h
call 00007F0F90A2CCB9h
push esi
mov esi, eax
or esi, eax
mov eax, esi
pop esi
jne 00007F0F90A31DB2h

Instruction
pushad
push 00000000h
mov dword ptr [esp], edi
xor edi, edi
or edi, dword ptr [ebx+0041856Bh]
mov eax, edi
pop edi
push edx
add dword ptr [esp], 40h
sub dword ptr [esp], edx
push ebx
mov dword ptr [esp], 00001000h
push edi
sub dword ptr [esp], edi
xor dword ptr [esp], eax
push 00000000h
call dword ptr [ebx+0045D014h]
mov dword ptr [ebp-04h], ecx
and ecx, 00000000h
xor ecx, eax
and edi, 00000000h
or edi, ecx
mov ecx, dword ptr [ebp-04h]
push eax
sub eax, dword ptr [esp]
or eax, edi
and dword ptr [ebx+0041809Bh], 00000000h
xor dword ptr [ebx+0041809Bh], eax
pop eax
cmp ebx, 00000000h
jbe 00007F0F90A31D8Eh
add dword ptr [ebx+004180F7h], ebx
add dword ptr [ebx+00418633h], ebx
mov dword ptr [ebp-04h], edx
sub edx, edx
xor edx, dword ptr [ebx+004180F7h]
mov esi, edx
mov edx, dword ptr [ebp-04h]
push edi
xor edi, dword ptr [esp]
xor edi, dword ptr [ebx+0041856Bh]
and ecx, 00000000h
or ecx, edi
pop edi
cld
rep movsb
push ebx
mov dword ptr [eax+eax], 00000000h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x17000	0x51	.data
IMAGE_DIRECTORY_ENTRY_IMPORT	0x5d050	0x64	.data
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_IAT	0x5d000	0x50	.data
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.code	0x1000	0x15966	0x15a00	False	0.70799087789	data	6.48337924377	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x17000	0x51	0x200	False	0.140625	data	0.863325225156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rdata	0x18000	0x44c5f	0x1800	False	0.13330078125	data	0.926783139034	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.data	0x5d000	0x250	0x400	False	0.2900390625	data	2.96075631554	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Imports

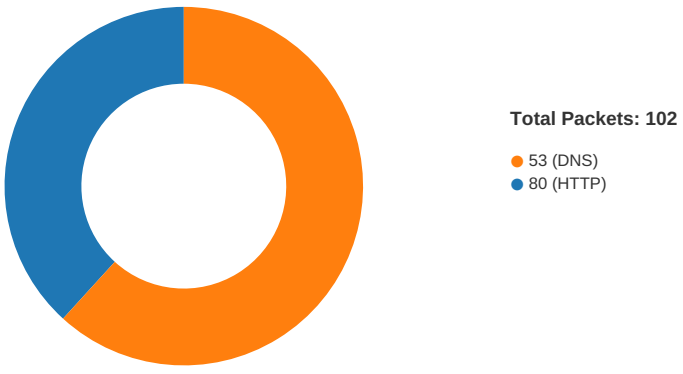
DLL	Import
user32.dll	GetActiveWindow, CheckDlgButton, CheckMenuItem, CheckRadioButton, CheckMenuRadioItem
kernel32.dll	GetProcAddress, LoadLibraryA, VirtualProtect, VirtualAlloc, lstrlenA, GetCurrentThreadId, GetCurrentProcess, GetCurrentThread, Module32FirstW
ole32.dll	OleInitialize
comctl32.dll	DPA_Sort

Exports

Name	Ordinal	Address
StartService	1	0x1000b959

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:56:12.096725941 CEST	49731	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:12.096864939 CEST	49732	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:13.261219978 CEST	49731	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:13.261276007 CEST	49732	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:13.731535912 CEST	49733	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:13.732633114 CEST	49734	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:14.827692032 CEST	49733	80	192.168.2.3	185.243.114.196

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:56:14.827832937 CEST	49734	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:15.359524965 CEST	49731	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:15.359533072 CEST	49732	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:16.839679003 CEST	49734	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:16.839688063 CEST	49733	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:19.375983953 CEST	49745	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:20.386806965 CEST	49745	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:20.862612009 CEST	49748	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:21.871412039 CEST	49748	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:22.387044907 CEST	49745	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:23.887120962 CEST	49748	80	192.168.2.3	185.243.114.196
Apr 6, 2021 09:56:49.986181021 CEST	49758	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:49.987652063 CEST	49759	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:50.009907007 CEST	49760	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:50.010023117 CEST	49761	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:50.998749971 CEST	49761	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:50.998788118 CEST	49758	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:51.000185013 CEST	49759	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:51.014389992 CEST	49760	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:52.998915911 CEST	49761	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:53.014547110 CEST	49758	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:53.014547110 CEST	49760	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:53.014780998 CEST	49759	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:57.001131058 CEST	49764	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:57.032944918 CEST	49766	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:57.036500931 CEST	49765	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:57.999392033 CEST	49764	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:58.046267033 CEST	49766	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:58.046264887 CEST	49765	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:56:59.999651909 CEST	49764	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:57:00.046372890 CEST	49765	80	192.168.2.3	185.186.244.95
Apr 6, 2021 09:57:00.046591043 CEST	49766	80	192.168.2.3	185.186.244.95

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:54:54.504206896 CEST	50200	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:54:54.564409018 CEST	53	50200	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:00.146251917 CEST	51281	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:00.206820965 CEST	53	51281	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:20.537797928 CEST	49199	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:20.586859941 CEST	53	49199	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:22.196136951 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:22.242232084 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:23.715821981 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:23.776586056 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:24.581485033 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:24.664185047 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:25.655771017 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:25.705579042 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:25.839536905 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:25.890918016 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:25.965971947 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:26.023046970 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:27.071768999 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:27.078222990 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:27.119158030 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:27.126667976 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:27.166656971 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:27.212841034 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:28.969212055 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:29.026247978 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:29.067358971 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:29.113094091 CEST	53	60100	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:55:29.402494907 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:29.462807894 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:30.096946955 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:30.100956917 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:30.146420956 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:30.150290966 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:41.038669109 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:41.084599972 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:48.581273079 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:48.630168915 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:52.820933104 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:52.877217054 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:53.718832970 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:53.775741100 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:54.796432018 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:54.842394114 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:56.277920961 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:56.323849916 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 09:55:58.292025089 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:55:58.337914944 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:00.371872902 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:00.421405077 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:01.230736017 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:01.278012037 CEST	53	57568	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:02.307972908 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:02.353768110 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:10.400521040 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:10.454762936 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:12.005079985 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:12.081111908 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:13.645559072 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:13.691240072 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:13.862624884 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:13.919054031 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:14.072062016 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:14.118011951 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:14.542340994 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:14.590416908 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:15.046813965 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:15.092739105 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:15.614095926 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:15.668504953 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:15.752041101 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:15.814610958 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:16.302881956 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:16.357342005 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:17.159584045 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:17.214279890 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:18.437560081 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:18.483690977 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:19.104331970 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:19.153104067 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:19.574176073 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:19.630949020 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:20.500962973 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:20.605565071 CEST	53	64910	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:21.310638905 CEST	52123	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:21.368184090 CEST	53	52123	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:23.657238960 CEST	56130	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:23.715796947 CEST	53	56130	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:23.761136055 CEST	56338	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:23.807647943 CEST	53	56338	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:26.433443069 CEST	59420	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:26.487623930 CEST	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 09:56:27.934998035 CEST	58784	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:27.985817909 CEST	53	58784	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:34.248287916 CEST	63978	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:34.294377089 CEST	53	63978	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:39.853234053 CEST	62938	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:39.899269104 CEST	53	62938	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:48.560122967 CEST	55708	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:48.614381075 CEST	53	55708	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:49.841717005 CEST	56803	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:49.925148010 CEST	57145	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:49.982492924 CEST	53	57145	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:49.996510029 CEST	53	56803	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:51.002130032 CEST	55359	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:51.048753977 CEST	53	55359	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:51.901644945 CEST	58306	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:51.965435028 CEST	53	58306	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:59.034034967 CEST	64124	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:59.082752943 CEST	53	64124	8.8.8.8	192.168.2.3
Apr 6, 2021 09:56:59.874128103 CEST	49361	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:56:59.922846079 CEST	53	49361	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:04.025763988 CEST	63150	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:04.051103115 CEST	53279	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:04.071840048 CEST	53	63150	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:04.105596066 CEST	53	53279	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:09.808339119 CEST	56881	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:09.858160019 CEST	53	56881	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:10.616043091 CEST	53642	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:10.661824942 CEST	53	53642	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:11.382510900 CEST	55667	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:11.439739943 CEST	53	55667	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:12.661437035 CEST	54833	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:12.708245039 CEST	53	54833	8.8.8.8	192.168.2.3
Apr 6, 2021 09:57:13.861326933 CEST	62476	53	192.168.2.3	8.8.8.8
Apr 6, 2021 09:57:13.907584906 CEST	53	62476	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 6, 2021 09:55:27.071768999 CEST	192.168.2.3	8.8.8.8	0xf61	Standard query (0)	login.microsoftonline.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:12.005079985 CEST	192.168.2.3	8.8.8.8	0xfc99	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:13.645559072 CEST	192.168.2.3	8.8.8.8	0x5829	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:26.433443069 CEST	192.168.2.3	8.8.8.8	0x137f	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:27.934998035 CEST	192.168.2.3	8.8.8.8	0xaffc	Standard query (0)	under17.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:49.841717005 CEST	192.168.2.3	8.8.8.8	0x4c0b	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:49.925148010 CEST	192.168.2.3	8.8.8.8	0xa464	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:04.025763988 CEST	192.168.2.3	8.8.8.8	0x7d00	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:04.051103115 CEST	192.168.2.3	8.8.8.8	0x4ca0	Standard query (0)	urs-world.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:55:27.119158030 CEST	8.8.8.8	192.168.2.3	0xf61	No error (0)	login.microsoftonline.com	a.privatelink.msidentity.com		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:55:27.119158030 CEST	8.8.8.8	192.168.2.3	0xf61	No error (0)	a.privatelink.msidentity.com	prda.aadg.msidentity.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 6, 2021 09:55:27.119158030 CEST	8.8.8.8	192.168.2.3	0xf61	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:55:27.212841034 CEST	8.8.8.8	192.168.2.3	0x17ca	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:55:30.146420956 CEST	8.8.8.8	192.168.2.3	0xb8d8	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Apr 6, 2021 09:56:12.081111908 CEST	8.8.8.8	192.168.2.3	0xfc99	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:13.691240072 CEST	8.8.8.8	192.168.2.3	0x5829	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:26.487623930 CEST	8.8.8.8	192.168.2.3	0x137f	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:27.985817909 CEST	8.8.8.8	192.168.2.3	0xaffc	No error (0)	under17.com		185.243.114.196	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:49.982492924 CEST	8.8.8.8	192.168.2.3	0xa464	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 6, 2021 09:56:49.996510029 CEST	8.8.8.8	192.168.2.3	0x4c0b	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:04.071840048 CEST	8.8.8.8	192.168.2.3	0x7d00	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)
Apr 6, 2021 09:57:04.105596066 CEST	8.8.8.8	192.168.2.3	0x4ca0	No error (0)	urs-world.com		185.186.244.95	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

System Behavior

Analysis Process: loaddll32.exe PID: 5452 Parent PID: 5576

General

Start time:	09:55:00
Start date:	06/04/2021
Path:	C:\Windows\System32\loaddll32.exe
Wow64 process (32bit):	true
Commandline:	loaddll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll'
Imagebase:	0x3d0000
File size:	116736 bytes
MD5 hash:	542795ADF7CC08EFCF675D65310596E8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.318966853.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.318950554.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.319029773.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.318997670.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.401164058.0000000003A2D000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.318987145.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.480876876.000000000392F000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000001.00000003.318925659.0000000003B2B000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000001.00000002.487763309.0000000002ED0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 4904 Parent PID: 5452

General

Start time:	09:55:00
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /C rundll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll',#1
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 2628 Parent PID: 5452

General

Start time:	09:55:01
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe C:\Users\user\Desktop\0204_1.gif.dll,StartService
Imagebase:	0xc00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000004.00000002.248258066.0000000000BD0000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 68 Parent PID: 4904

General

Start time:	09:55:01
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	rundll32.exe 'C:\Users\user\Desktop\0204_1.gif.dll',#1
Imagebase:	0xc00000
File size:	61952 bytes
MD5 hash:	D7CA562B0DB4F4DD0F03A89A1FDAD63D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323251536.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif_1, Description: Yara detected Ursnif, Source: 00000005.00000002.486714562.0000000000BE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.480525805.0000000004DAF000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323328029.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323362066.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323281366.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323298116.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.404525963.0000000004EAD000.00000004.00000040.sdmp, Author: Joe Security • Rule: JoeSecurity_Ursnif, Description: Yara detected Ursnif, Source: 00000005.00000003.323337362.0000000004FAB000.00000004.00000040.sdmp, Author: Joe Security

Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6664 Parent PID: 792

General

Start time:	09:55:22
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62f200000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6708 Parent PID: 6664

General

Start time:	09:55:23
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:17410 /prefetch:2
Imagebase:	0x20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6972 Parent PID: 6664

General

Start time:	09:55:27
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6664 CREDAT:82952 /prefetch:2
Imagebase:	0x20000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6780 Parent PID: 792

General

Start time:	09:56:09
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62f200000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 1268 Parent PID: 6780

General

Start time:	09:56:09
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 5188 Parent PID: 6780

General

Start time:	09:56:11
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6780 CREDAT:17414 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 6384 Parent PID: 792

General

Start time:	09:56:47
Start date:	06/04/2021
Path:	C:\Program Files\internet explorer\iexplore.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Internet Explorer\iexplore.exe' -Embedding
Imagebase:	0x7ff62f200000
File size:	823560 bytes
MD5 hash:	6465CB92B25A7BC1DF8E01D8AC5E7596
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: iexplore.exe PID: 3360 Parent PID: 6384

General

Start time:	09:56:48
Start date:	06/04/2021
Path:	C:\Program Files (x86)\Internet Explorer\iexplore.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Internet Explorer\IEXPLORE.EXE' SCODEF:6384 CREDAT:17410 /prefetch:2
Imagebase:	0x210000
File size:	822536 bytes
MD5 hash:	071277CC2E3DF41EEEA8013E2AB58D5A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis